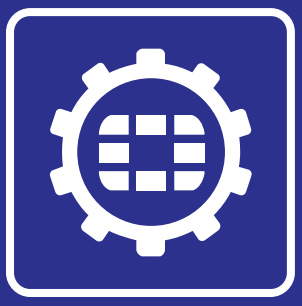


FORTINET

FortiOS™ Handbook - System Administration

VERSION 6.0.3

FORTIOS VERSION 6.0

FORTINET DOCUMENT LIBRARY

https://docs.fortinet.com

FORTINET VIDEO GUIDE

https://video.fortinet.com

FORTINET KNOWLEDGE BASE

http://kb.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTINET COOKBOOK

http://cookbook.fortinet.com

FORTINET NSE INSTITUTE (TRAINING)

https://training.fortinet.com/

FORTIGUARD CENTER

https://fortiguard.com

FORTICAST

http://forticast.fortinet.com

END USER LICENSE AGREEMENT AND PRIVACY POLICY

https://www.fortinet.com/doc/legal/EULA.pdf

https://www.fortinet.com/corporate/about-us/privacy.html

FEEDBACK

Email: techdocs@fortinet.com

November 16, 2018

FortiOS™ Handbook - System Administration

01-603-481094-20181116

TABLE OF CONTENTS

Change log

Date	Change description
November 16, 2018	Minor fixes.
August 17, 2018	Corrections to "SNMP" on page 22.
July 27, 2018	Corrections to "Session helpers" on page 56.
July 26, 2018	FortiOS 6.0.2 document release. Minor updates.
June 5, 2018	FortiOS 6.0.1 document release. Minor updates.
March 29, 2018	FortiOS 6.0 document release. See "What's new in FortiOS 6.0" on page 8. Note that the Central Management section has moved to the Fortinet Security Fabric document.

Welcome and thank you for selecting Fortinet products for your network protection.

This guide explains system administration features on your FortiGate as well as basic configuration tasks, best practices, and more advanced configuration options.

How this guide is organized

This guide contains the following sections:

- What's New in FortiOS 6.0 informs you about new system administration features in FortiOS 6.0.
- Administrators describes the tasks to add and secure administrative access to a FortiGate.
- Monitoring discusses the various methods of monitoring both your FortiGate and network traffic through a range of different tools available within FortiOS.
- Replacement messages explains how to view and customize replacement messages on your FortiGate.
- Administration for schools shares basic practices administrators in school systems can employ .
- PPTP and L2TP contains information on configuring PPTP and L2TP VPNs as well as PPTP passthrough.
- Session helpers explains how to use session helpers to analyze data in the packet bodies of some protocols and make adjustments to allow those protocols to send packets through the firewall.
- Advanced concepts describes more involved administrative topics to enhance network security and traffic efficiency.

What's new in FortiOS 6.0

The following list contains new system administration features added in FortiOS 6.0. Click on a link to navigate to that section for further information.

- Updates to "Administrator profiles" on page 9
- "Restrict local admin authentication when remote authentication server is running" on page 16
- "FortiToken extension to comply with PCI 3.2" on page 20
- "Multi-dimension tagging" on page 77

Administrators

By default, the FortiGate has a super administrator account, called `admin`, which can't be deleted. Additional administrators can be added for various functions, each with a unique user name, password, and set of access privileges.

The following sections explain how to add and secure administrative access to a FortiGate:

Administrator profiles

Administrator profiles define what the administrator can do when logged into the FortiGate. When you set up an administrator account, you also assign an administrator profile dictating what the administrator sees. Depending on the nature of the administrator's work, access level or seniority, you can allow them to view and configure as much, or as little, as required.

super_admin profile

This profile has access to all components of FortiOS, including the ability to add and remove other system administrators. For certain administrative functions, such as backing up and restoring the configuration, super_admin access is required. To ensure that there is always a method to administer the FortiGate, the super_admin profile can't be deleted or modified.

Lower level administrator profiles can't backup or restore the FortiOS configuration.

The super_admin profile is used by the default `admin` account. We recommend that you add a password and rename this account once you have set up your FortiGate. In order to rename the default account, a second admin account is required. For more information, see "Adding a local administrator" on page 10.

Creating profiles

To configure administrator profiles, go to **System > Admin Profiles** and select **Create New**.

On the **New Admin Profile** page, select the access permissions for the admin profile you are creating. For example, you can configure a profile so that the administrator can only read/write **Firewall** configuration, which

includes firewall policies, addresses, services, schedules, packet capture, and some other parts of the FortiGate configuration. Any other aspects of the FortiGate configuration, including VPNs and security profiles, would be hidden from this administrator.

Access control can also be set to **Custom** for some features. This allows for more granular control of administrator access. Using the **Firewall** example, you can set access to **Custom** and then select separate **Read/Write** privileges for **Policy**, **Address**, **Service**, and **Schedule**.

Administrator timeout override per access profile

You can configure administrator profiles to increase inactivity timeout and facilitate use of the GUI for central monitoring. This feature allows the `admintimeout` value, under `config system accprofile`, to be overridden per access profile.

Note that you can set this on a per-profile basis, to avoid the option from being unintentionally set globally.

CLI Syntax - Configure admin timeout

```
config system accprofile
   edit <name>
      set admintimeout-override {enable | disable}
      set admintimeout <0-480> - (default = 10, 0 = unlimited)
   next
end
```

Adding a local administrator

Only administrators with read-write privileges for **User & Device** can create a new administrator account.

To add an administrator - GUI

1. Go to **System > Administrators**.
2. Select **Create New > Administrator**.
3. Add a **Username** for the administrator.

Don't include the characters `<>()#"'` in the administrator's name . Using these characters in the administrator account name can result in a cross site scripting (XSS) vulnerability.

4. Set **Type** to **Local User**.
5. Enter the **Password** for the user. This may be a temporary password that the administrator can change later. Passwords can be up to 256 characters in length. For more information on passwords, see the Passwords discussion in the Getting Started chapter.
6. Determine if you need to enable security options: **SMS**, **Two-factor Authentication**, **Restrict login to trusted hosts**, **Restrict admin to guest account provisioning only**.
7. Select **OK**.

You can configure guest management administrator's through the GUI. To create the user group to be used for guest user accounts, go to Managing Guest Access in the Authentication chapter.

To add an administrator - CLI

```
config system admin
   edit <admin_name>
      set password <password>
      set accprofile <profile_name>
      set guest-auth {enable | disable}
      set user-groups <group-name>
end
```

The CLI command `set user-groups` can only be used when `guest-auth` is set to `enable`.

LDAP authentication for administrators

Administrators can use remote authentication, such as LDAP, to connect to the FortiGate.

To do this, you must follow these three steps:

- configure the LDAP server
- add the LDAP server to a user group
- configure the administrator account

Configure the LDAP server

First set up the LDAP server as you normally would, and include a group to bind to.

To configure the LDAP server - GUI

1. Go to **User & Device > LDAP Servers** and select **Create New**.
2. Enter a **Name** for the server.
3. Enter the **Server IP** address or name.
4. Enter the **Common Name Identifier** and **Distinguished Name**.
5. Set the **Bind Type** to **Regular** and enter the **Username** and **Password**.
6. Select **OK**.

To configure the LDAP server - CLI

```
config user ldap
   edit <ldap_server_name>
      set server <server_ip>
      set cnid cn
      set dn DC=XYZ,DC=COM
      set type regular
      set user name CN=Administrator,CN=Users,DC=XYZ,DC=COM
      set password <password>
      set member-attr <group_binding>
```

```
end
```

Add the LDAP server to a user group

Next, create a user group that will include the LDAP server that was created above.

To create a user group - GUI

1. Go to **User & Device > User Groups** and select **Create New**.
2. Enter a **Name** for the group.
3. In the section labeled **Remote groups**, select **Create New**.
4. Select the **Remote Server** from the drop-down list.
5. Select **OK**.

To create a user group - CLI

```
config user group
   edit <group_name>
      config match
         edit 1
            set server-name <LDAP_server>
            set group-name <group_name>
      end
   end
```

Configure the administrator account

Now you can create a new administrator, where rather than entering a password, you will use the new user group and the wildcard option for authentication.

To create an administrator - GUI

1. Go to **System > Administrators** and select **Create New**.
2. In the **Administrator** field, enter the name for the administrator.
3. For **Type**, select **Match a user on a remote server group**.
4. Select the **User Group** created above from the drop-down list.
5. Select **Wildcard**. The Wildcard option allows for LDAP users to connect as this administrator.
6. Select an **Admin Profile**.
7. Select **OK**.

To create an administrator - CLI

```
config system admin
   edit <admin_name>
      set remote-auth enable
      set accprofile super_admin
      set wild card enable
      set remote-group ldap
   end
```

Other methods of administrator authentication

Admin accounts can use a variety of methods for authentication, including RADIUS, TACACS+, and PKI.

RADIUS authentication for administrators

If you want to use a RADIUS server to authenticate administrators, you must:

- configure the FortiGate to access the RADIUS server
- create the RADIUS user group
- configure an administrator to authenticate with a RADIUS server.

TACACS+ authentication for administrators

If you want to use a TACACS+ server to authenticate administrators, you must:

- configure the FortiGate to access the TACACS+ server
- create a TACACS+ user group
- configure an administrator to authenticate with a TACACS+ server.

PKI certificate authentication for administrators

To use PKI authentication for an administrator, you must:

- configure a PKI user
- create a PKI user group
- configure an administrator to authenticate with a PKI certificate.

Administrator lockout

By default, the FortiGate sets the number of password retries at three, allowing the administrator a maximum of three attempts to log into their account before locking the account for a set amount of time.

Both the number of attempts (`admin-lockout-threshold`) and the wait time before the administrator can try to enter a password again (`admin-lockout-duration`) can be configured within the CLI.

To configure the lockout options:

```
config system global
   set admin-lockout-threshold <failed_attempts>
   set admin-lockout-duration <seconds>
end
```

The default value of `admin-lockout-threshold` is 3 and the range of values is between 1 and 10. The `admin-lockout-duration` is set to 60 seconds by default and the range of values is between 1 and 4294967295 seconds.

Keep in mind that the higher the lockout threshold, the higher the risk that someone may be able to break into the FortiGate.

Example:

To set the `admin-lockout-threshold` to one attempt and the `admin-lockout-duration` to a five minute duration before the administrator can try to log in again, enter the commands:

```
config system global
   set admin-lockout-threshold 1
   set admin-lockout-duration 300
end
```

If the time span between the first failed login attempt and the `admin-lockout-threshold` failed login attempt is less than `admin-lockout-duration`, the lockout will be triggered.

Monitoring administrators

You can view the administrators logged in using the **System Information** widget on the Dashboard. The **Current Administrator** row that shows the administrator logged in and the total number of administrators logged in. Selecting **Details** displays the administrators, where they are logging in from and how (CLI, GUI) and when they logged in.

You are also able to monitor the activities the administrators perform on the FortiGate using the event logging. Event logs include a number of options to track configuration changes.

To set logging - GUI

1. Go to **Log & Report > Log Settings**.
2. Under **Event Logging**, select **Customize** and ensure **System activity event** is selected.
3. Select **Apply**.

To set logging - CLI

```
config log eventfilter
   set event enable
   set system enable
end
```

To view the logs go to **Log & Report > System Events**.

Management access

Management access defines how administrators are able to log on to the FortiGate. In NAT mode, access is configured for each of the FortiGate's interfaces, using the interface's IP to connect. In transparent mode, a single management IP address is configured to allow access.

Management access can be via HTTP, HTTPS, Telnet, or SSH sessions. HTTPS and SSH are preferred as they are more secure. The management computer must connect to an interface that permits management access and its IP address must be on the same network. If you are using VDOMs, an administrator who is restricted to a specific VDOM must use a computer that connects to an interface on that VDOM.

You can allow remote administration of the FortiGate; however, it is not recommended, since it could compromise the security of the FortiGate. If you require remote administration, the following precautions can be taken to improve the security of a FortiGate:

- Use secure administrator passwords.
- Change these passwords regularly.
- Enable two-factor authentication for administrators.
- Enable secure administrative access to this interface using only HTTPS or SSH.
- Use Trusted Hosts to limit where the remote access can originate from.
- Don't change the system idle timeout from the default value of 5 minutes.

Security precautions

One potential point of a security breach is at the management computer. Administrators who leave their workstations for a prolonged amount of time while staying logged into the GUI or CLI leave the firewall open to malicious intent.

When logging in using a local admin with the default or empty password, a warning prompt will appear upon login. Admins will be logged out if they have no permissions.

Restrict logins from trusted hosts

Setting up trusted hosts for an administrator limits the addresses from where they can log into FortiOS. The trusted hosts configuration applies to most forms of administrative access including HTTPS, SSH, and SNMP. When you identify a trusted host for an administrator account, FortiOS accepts that administrator’s login only from one of the trusted hosts. A login, even with proper credentials, from a non-trusted host is dropped.

Even if you have configured trusted hosts, if you have enabled ping administrative access on a FortiGate interface, it will respond to ping requests from any IP address.

To identify trusted hosts, go to **System > Administrators**, edit the administrator account, enable **Restrict login to trusted hosts**, and add up to ten trusted host IP addresses.

To add two trusted hosts from the CLI:

```
config system admin
   edit <administrator-name>
      set trustedhost1 172.25.176.23 255.255.255.255
      set trustedhost2 172.25.177.0 255.255.255.0
   end
```

Trusted host IP addresses can identify individual hosts or subnets. Just like firewall policies, FortiOS searches through the list of trusted hosts in order and acts on the first match it finds. When you configure trusted hosts, start by adding specific addresses at the top of the list. Follow with more general IP addresses. You don't have to add addresses to all of the trusted hosts as long as all specific addresses are above all of the 0.0.0.0 0.0.0.0 addresses.

Prevent concurrent administrator sessions

Concurrent administrator sessions occur when multiple people concurrently access the FortiGate using the same administrator account. This is allowed by default. If you wish to prevent this behavior go to **System > Settings** and disable **Allow multiple concurrent sessions for each administrator**.

From the CLI:

```
config system global
   set admin-concurrent disable
end
```

Note, if you disable concurrent sessions for an administrator, you will be allowed only one session with the same username even if it is from the same IP.

Restrict local admin authentication when remote authentication server is running

The following command can be enabled so that whenever any remote server (TACACS, LDAP, or RADIUS) is up and running, any local admin authentication will be blocked. Local admins will be allowed access only if no remote server is detected.

Syntax:

```
config system global
   set admin-restrict-local {enable | disable}- (Default is set to disable)
end
```

Segregate administrative roles

To minimize the effect of an administrator causing errors to the FortiGate configuration and possibly jeopardizing the network, create individual administrative roles where none of the administrators have super_admin permissions. For example, one account is used solely to create security policies, another for users and groups, another for VPN, and so on.

SSH log in time out

You can take up to 120 seconds to log into the FortiGate when using SSH. You can use the following CLI command to reduce this time and enhance security:

```
config system global
   set admin-ssh-grace-time <number_of_seconds>
end
```

The range can be between 10 and 3600 seconds.

HTTPS redirect

When configuring the Administration Settings (found at **System > Settings**), you can also enable HTTP to **Redirect to HTTPS**. When enabled, if a administrator tries to connect to an interface using HTTP, this traffic will be automatically redirected to use HTTPS instead for a more secure connection.

Administrator log in disclaimers

FortiOS can display a disclaimer before or after logging into the GUI or CLI (or both). In either case the administrator must read and accept the disclaimer before they can proceed.

Use the following command to display a disclaimer before logging in:

```
config system global
   set pre-login-banner enable
end
```

Use the following command to display a disclaimer after logging in:

```
config system global
   set post-login-banner enable
end
```

You can customize the replacement messages for these disclaimers by going to **System > Replacement Messages**. Select **Extended View** to view and edit the **Administrator** replacement messages.

From the CLI:

```
config system replacemsg admin pre_admin-disclaimer-text
config system replacemsg admin post_admin-disclaimer-text
```

Disable the console interface

You can disable your FortiGate's console interface to prevent any unwanted login attempts:

```
config system console
   set login disable
end
```

Disable other interfaces

If any of the interfaces on the FortiGate aren't being used, disable traffic on that interface. This avoids someone plugging in network cables and potentially causing network bypass or loop issues.

To disable an interface - GUI

1. Go to **Network > Interfaces**.
2. Select the interface from the list and select **Edit**.
3. For **Administrative Access**, select **Down**.
4. Select **OK**.

To disable an interface - CLI

```
config system interface
   edit <interface_name>
      set status down
end
```

Self-signed GUI certificates

For increased security, the self-sign certificate is the default GUI certificate, if the BIOS certificate is using SHA-1.

Monitoring

With network administration, the first step is installing and configuring the FortiGate to be the protector of the internal network. Once the system is running efficiently, the next step is to monitor the system and network traffic. When a threat or vulnerability is discovered, you can make configuration changes as necessary.

This chapter discusses the various methods of monitoring both the FortiGate and the network traffic through a range of different tools available within FortiOS.

This section includes the topics:

Dashboard

The FortiOS dashboard provides real-time system information presented in a network operations center (NOC) view with a focus on alerts. By default, the dashboard displays key statistics for the FortiGate, such as memory and CPU status, port health, whether they are up or down and their throughput. Widgets are interactive. By clicking or hovering over most widgets, you can get additional information or follow links to other pages.

The dashboard and its widgets include:

- Multiple dashboard support.
- VDOM and global dashboards.
- Widget resize control.
- Notifications on the top header bar.

For more information, see the Dashboard discussion in the Getting Started chapter of the Handbook.

Monitor menus

The **Monitor** menus enable you to view session and policy information and other activity occurring on your FortiGate unit. The monitors provide the details of user activity, traffic and policy usage to show live activity. Monitors are available for DHCP, routing, security policies, traffic shaping, load balancing, security features, VPN, users, and WiFi.

Logging

FortiOS provides a robust logging environment that enables you to monitor, store, and report traffic information and FortiGate events, including attempted log ins and hardware status. Depending on your requirements, you can log to a number of different hosts.

To configure logging in the web-based manager, go to **Log & Report > Log Settings**.

To configure logging in the CLI use the commands `config log <log_location>`.

For details on configuring logging see the Logging and Reporting Guide.

If you will be using several FortiGate units, you can also use a FortiAnalyzer unit for logging. For more information, see the FortiAnalyzer Administration Guide.

Syslog server

An industry standard for collecting log messages, for off-site storage. In the web-based manager, you are able to send logs to a single syslog server, however in the CLI you can configure up to three syslog servers where you can also use multiple configuration options. For example, send traffic logs to one server, antivirus logs to another. The FortiGate unit sends Syslog traffic over UDP port 514. Note that if a secure tunnel is configured for communication to a FortiAnalyzer unit, then Syslog traffic will be sent over an IPsec connection, using UPD 500/4500, Protocol IP/50.

To configure a Syslog server in the web-based manager, go to **Log & Report > Log Settings**. In the CLI use the commands:

```
config log syslogd setting
   set status enable
   set server <IP address or FQDN of syslog server>
end
```

Further options are available when enabled to configure a different port, facility and server IP address.

For Syslog traffic, you can identify a specific port/IP address for logging traffic. Configuration of these services is performed in the CLI, using the command `set source-ip`. When configured, this becomes the dedicated port to send this traffic over.

For example, to set the source IP of a Syslog server to be on the DMZ1 port with an IP of 192.168.4.5, the commands are:

```
config log syslogd setting
   set status enable
   set source-ip 192.168.4.5
end
```

FortiToken extension to comply with PCI 3.2

For FortiToken to be PCI 3.2 compliant, multi-factor authentication with FortiOS can be globally enforced for all login methods under `config system global`.

When `multi-factor-authentication` is set to `mandatory`, the system will collect and log each factor (username, password, and OTP) after authentication.

Note that even if a user is not configured with two-factor authentication, an empty OTP (or any OTP entered) will make second factor authentication pass.

Syntax:

```
config system global
   set multi-factor-authentication {optional | mandatory} - (Default is set to optional)
end
```

Alert email

As an administrator, you want to be certain you can respond quickly to issues occurring on your network or on the FortiGate unit. Alert emails provide an efficient and direct method of notifying an administrator of events. By configuring alert messages, you can define the threshold when a problem becomes critical and needs attention. When this threshold is reached, the FortiGate unit will send an email to one or more individuals, notifying them of the issue.

In the following example, the FortiGate unit is configured to send email to two administrators (admin1 and admin2) when multiple intrusions are detected every two minutes. The FortiGate unit has its own email address on the mail server.

To configure the email service

1. Go to **System > Advanced**.
2. In the **Email Service**, enable **Use Custom Email Server**, complete the following and select **Apply**:

SMTP Server	Enter the address or name of the email server. For example, `smtp.example.com`.
Default Reply To	Enter an email address to associate with the alert email. This field is optional. If you enter an email address here, it overrides the email address entered when configuring alert email in **Log & Report > Email Alert Settings**.
Authentication	Enable authentication if required by the email server.
Security mode	Choose between *None*, *SMTPS* or *STARTTLS*
Port	25

To configure alert email - GUI

1. Go to **Log & Report > Email Alert Settings**.
2. Enter the information:

Email from	fortigate@example.com
Email to	admin1@example.com admin2@example.com

3. For the **Interval Time**, enter 2.
4. Select **Intrusion Detected**.
5. Select **Apply**.

To configure alert email - CLI

```
config system email-server
   set port 25
   set server smtp.example.com
   set authenticate enable
   set username FortiGate
   set password *************
end
config alertemail setting
   set username fortigate@example.com
   set mailto1 admin1@example.com
   set mailto2 admin2@example.com
   set filter category
   set IPS-logs enable
end
```

SNMP

Simple Network Management Protocol (SNMP) enables you to monitor hardware on your network. You can configure the hardware, such as the FortiGate SNMP agent, to report system information and send traps (alarms or event messages) to SNMP managers. An SNMP manager, or host, is a typically a computer running an application that can read the incoming trap and event messages from the agent and send out SNMP queries to the SNMP agents. A FortiManager unit can act as an SNMP manager to one or more FortiGate units. FortiOS supports SNMP using IPv4 and IPv6 addressing.

By using an SNMP manager, you can access SNMP traps and data from any FortiGate interface or VLAN subinterface configured for SNMP management access. Part of configuring an SNMP manager is to list it as a host in a community on the FortiGate unit it will be monitoring. Otherwise, the SNMP monitor will not receive any traps from that FortiGate unit or be able to query that unit.

The FortiGate SNMP implementation is read-only. SNMP v1, v2c, and v3 compliant SNMP managers have read-only access to FortiGate system information through queries and can receive trap messages from the FortiGate unit.

To monitor FortiGate system information and receive FortiGate traps, you must first compile the Fortinet and FortiGate Management Information Base (MIB) files. A MIB is a text file that describes a list of SNMP data objects that are used by the SNMP manager. These MIBs provide information the SNMP manager needs to interpret the SNMP trap, event, and query messages sent by the FortiGate unit SNMP agent.

FortiGate core MIB files are available for download by going to **System > SNMP** and selecting the download link on the page.

The Fortinet implementation of SNMP includes support for most of RFC 2665 (Ethernet-like MIB) and most of RFC 1213 (MIB II). For more information, see “Fortinet MIBs”. RFC support for SNMP v3 includes Architecture for SNMP Frameworks (RFC 3411), and partial support of User-based Security Model (RFC 3414).

SNMP traps alert you to events that occur such as a full log disk or a virus detected.

SNMP fields contain information about the FortiGate unit, such as CPU usage percentage or the number of sessions. This information is useful for monitoring the condition of the unit on an ongoing basis and to provide more information when a trap occurs.

The FortiGate SNMP v3 implementation includes support for queries, traps, authentication, and privacy. Authentication and encryption are configured in the CLI. See the `system snmp user` command in the FortiGate CLI Reference.

SNMP trap for bypass events

When bypass mode is enabled or disabled on FortiGate units that are equipped with bypass interfaces and support AMC modules, a new SNMP trap is generated and logs bypass events.

Implement SNMP support for NAT Session monitoring which includes new SNMP OIDs

FortiOS 6.0 implements a feature providing SNMP support for NAT session monitoring. The resulting new SNMP object identifier (OID) is:

FORTINET-FORTIGATE-MIB:fortinet.fnFortiGateMib.fgFirewall.fgFwIppools.fgFwIppTables.fgFwIppStatsTable.fgFwIppStatsEntry 1.3.6.1.4.1.12356.101.5.3.2.1.1

Additionally, there are eight other items:

.fgFwIppStatsName .1

.fgFwIppStatsType .2

.fgFwIppStatsStartIp .3

.fgFwIppStatsEndIp .4

.fgFwIppStatsTotalSessions .5

.fgFwIppStatsTcpSessions .6

.fgFwIppStatsUdpSessions .7

.fgFwIppStatsOtherSessions .8

SNMP configuration settings

Before a remote SNMP manager can connect to the FortiGate agent, you must configure one or more FortiGate interfaces to accept SNMP connections by going to **Network > Interfaces**. Select the interface and, in the **Administrative Access**, select **SNMP**.

For VDOMS, SNMP traps can only be sent on interfaces in the management VDOM. Traps cannot be sent over other interfaces outside the management VDOM.

To configure SNMP settings, go to **System > SNMP**.

SNMP Agent	Select to enable SNMP communication.
Description	Enter descriptive information about the FortiGate unit. The description can be up to 35 characters.

Location	Enter the physical location of the FortiGate unit. The system location description can be up to 35 characters long.
Contact	Enter the contact information for the person responsible for this FortiGate unit. The contact information can be up to 35 characters.
SNMP v1/v2c section To create a new SNMP community, see SNMP Community.	
Community Name	The name to identify the community.
Queries	Indicates whether queries protocols (v1 and v2c) are enabled or disabled. A green check mark indicates queries are enabled; a gray x indicates queries are disabled. If one query is disabled and another one enabled, there will still be a green check mark.
Traps	Indicates whether trap protocols (v1 and v2c) are enabled or disabled. A green check mark indicates traps are enabled; a gray x indicates traps are disabled. If one query is disabled and another one enabled, there will still be a green check mark.
Enable	Select the check box to enable or disable the community.
SNMP v3 section To create a new SNMP community, see SNMP Community page.	
User Name	The name of the SNMPv3 user
Security Level	The security level of the user
Notification Host	The IP address or addresses of the host
Queries	Indicates whether queries are enabled or disabled. A green check mark indicates queries are enabled; a gray x indicates queries are disabled
New SNMP Community page	
Community Name	Enter a name to identify the SNMP community
Hosts (section)	
IP Address	Enter the IP address and Identify the SNMP managers that can use the settings in this SNMP community to monitor the FortiGate unit. You can also set the IP address to 0.0.0.0 to so that any SNMP manager can use this SNMP community.
Delete	Removes an SNMP manager from the list within the **Hosts** section

Add	Select to add a blank line to the Hosts list. You can add up to eight SNMP managers to a single community.
Queries (section)	
Protocol	The SNMP protocol. In the v1 row, this means that the settings are for SNMP v1. In the v2c row, this means that the settings are for SNMP v2c.
Port	Enter the port number (161 by default) that the SNMP managers in this community use for SNMP v1 and SNMP v2c queries to receive configuration information from the FortiGate unit. Select the **Enable** check box to activate queries for each SNMP version. **Note:** The SNMP client software and the FortiGate unit must use the same port for queries.
Enable	Select to enable that SNMP protocol.
Traps (section)	
Protocol	The SNMP protocol. In the v1 row, this means that the settings are for SNMP v1. In the v2c row, this means that the settings are for SNMP v2c.
Local	Enter the remote port numbers (port 162 for each by default) that the FortiGate unit uses to send SNMP v1 or SNMP v2c traps to the SNMP managers in this community. Select the **Enable** check box to activate traps for each SNMP version. **Note:** The SNMP client software and the FortiGate unit must use the same port for traps.
Remote	Enter the remote port number (port 162 is default) that the FortiGate unit uses to send SNMP v1 or v2c traps to the SNMP managers in this community. **Note:** The SNMP client software and the FortiGate unit must use the same port for queries.
Enable	Select to activate traps for each SNMP version.
SNMP Event	Enable each SNMP event for which the FortiGate unit should send traps to the SNMP managers in this community. **CPU Over usage** traps sensitivity is slightly reduced, by spreading values out over 8 polling cycles. This prevents sharp spikes due to CPU intensive short-term events such as changing a policy. **Power Supply Failure** event trap is available only on some models. **AMC interfaces enter bypass mode** event trap is available only on models that support AMC modules.

Enable	Select to enable the SNMP event.
Create New SNMP V3 User	
User Name	Enter the name of the user.
Security Level	Select the type of security level the user will have.
Notification Host	Enter the IP address of the notification host. If you want to add more than one host, after entering the IP address of the first host, select the plus sign to add another host.
Enable Query	Select to enable or disable the query. By default, the query is enabled.
Port	Enter the port number in the field.
Events	Select the SNMP events that will be associated with that user.

Gigabit interfaces

When determining the interface speed of a FortiGate unit with a 10G interface, the IF-MIB.ifSpeed may not return the correct value. IF-MIB.ifSpeed is a 32-bit gauge used to report interface speeds in bits/second and cannot convert to a 64-bit value. The 32-bit counter wrap the output too fast to be accurate.

In this case, you can use the value ifHighSpeed. It reports interface speeds in megabits/second. This ensures that 10Gb interfaces report the correct value.

SNMP agent

You need to first enter information and enable the FortiGate SNMP Agent. Enter information about the FortiGate unit to identify it so that when your SNMP manager receives traps from the FortiGate unit, you will know which unit sent the information.

To configure the SNMP agent - GUI

1. Go to **System > SNMP**.
2. Select **Enable** for the **SNMP Agent**.
3. Enter a descriptive name for the agent.
4. Enter the location of the FortiGate unit.
5. Enter a contact or administrator for the SNMP Agent or FortiGate unit.
6. Select **Apply**.

To configure SNMP agent - CLI

```
config system snmp sysinfo
   set status enable
   set contact-info <contact_information>
   set description <description_of_FortiGate>
   set location <FortiGate_location>
end
```

SNMP community

An SNMP community is a grouping of devices for network administration purposes. Within that SNMP community, devices can communicate by sending and receiving traps and other information. One device can belong to multiple communities, such as one administrator terminal monitoring both a firewall SNMP and a printer SNMP community.

Add SNMP communities to your FortiGate unit so that SNMP managers can connect to view system information and receive SNMP traps.

You can add up to three SNMP communities. Each community can have a different configuration for SNMP queries and traps. Each community can be configured to monitor the FortiGate unit for a different set of events. You can also add the IP addresses of up to 8 SNMP managers to each community.

When the FortiGate unit is in virtual domain mode, SNMP traps can only be sent on interfaces in the management virtual domain. Traps cannot be sent over other interfaces.

To add an SNMP v1/v2c community - GUI

1. Go to **System > SNMP**.
2. In the **SNMP v1/v2c** area, select **Create New**.
3. Enter a **Community Name**.
4. Enter the IP address and Identify the SNMP managers that can use the settings in this SNMP community to monitor the FortiGate unit.
5. Select the interface if the SNMP manager is not on the same subnet as the FortiGate unit.
6. Enter the **Port** number that the SNMP managers in this community use for SNMP v1 and SNMP v2c queries to receive configuration information from the FortiGate unit. Select the **Enable** check box to activate queries for each SNMP version.
7. Enter the Local and Remote port numbers that the FortiGate unit uses to send SNMP v1 and SNMP v2c traps to the SNMP managers in this community.
8. Select the **Enable** check box to activate traps for each SNMP version.
9. Select **OK**.

To add an SNMP v1/v2c community - CLI

```
config system snmp community
   edit <index_number>
      set events <events_list>
      set name <community_name>
      set query-v1-port <port_number>
      set query-v1-status {enable | disable}
      set query-v2c-port <port_number>
      set query-v2c-status {enable | disable}
      set status {enable | disable}
      set trap-v1-lport <port_number>
      set trap-v1-rport <port_number>
      set trap-v1-status {enable | disable}
      set trap-v2c-lport <port_number>
      set trap-v2c-rport <port_number>
      set trap-v2c-status {enable | disable}
end
```

To add an SNMP v3 community - GUI

1. Go to **System > SNMP**.
2. In the **SNMP v3** area, select **Create New**.
3. Enter a **User Name**.
4. Select a **Security Level** and associated authorization algorithms.
5. Enter the IP address of the **Notification Host** SNMP managers that can use the settings in this SNMP community to monitor the FortiGate unit.
6. Enter the **Port** number that the SNMP managers in this community use to receive configuration information from the FortiGate unit. Select the **Enable** check box to activate queries for each SNMP version.
7. Select the **Enable** check box to activate traps.
8. Select **OK**.

To add an SNMP v3 community - CLI

```
config system snmp user
   edit <index_number>
      set security-level {auth-priv | auth-no-priv | no-auth-no-priv}
      set queries enable
      set query-port <port_number>
      set notify-hosts <ip_address>
      set events <event_selections>
end
```

Enabling on the interface

Before a remote SNMP manager can connect to the FortiGate agent, you must configure one or more FortiGate interfaces to accept SNMP connections.

To configure SNMP access - GUI

1. Go to **Network > Interfaces**.
2. Choose an interface that an SNMP manager connects to and select **Edit**.
3. In **Administrative Access**, select **SNMP**.
4. Select **OK**.

To configure SNMP access - CLI

```
config system interface
   edit <interface_name>
      set allowaccess snmp
end
```

If the interface you are configuring already has protocols that are allowed access, use the command `append allowaccess snmp` instead, or else the other protocols will be replaced. For more information, see Adding and removing options from lists.

Fortinet MIBs

The FortiGate SNMP agent supports Fortinet proprietary MIBs as well as standard RFC 1213 and RFC 2665 MIBs. RFC support includes support for the parts of RFC 2665 (Ethernet-like MIB) and the parts of RFC 1213 (MIB II) that apply to FortiGate unit configuration.

There are two MIB files for FortiGate units - the Fortinet MIB, and the FortiGate MIB. The Fortinet MIB contains traps, fields and information that is common to all Fortinet products. The FortiGate MIB contains traps, fields and information that is specific to FortiGate units. Each Fortinet product has its own MIB. If you use other Fortinet products you will need to download their MIB files as well. Both MIB files are used for FortiOS and FortiOS Carrier; there are no additional traps for the Carrier version of the operating system.

The Fortinet MIB and FortiGate MIB along with the two RFC MIBs are listed in tables in this section. To download the two FortiGate MIB files, visit the Fortinet Support website. The Fortinet MIB contains information for Fortinet products in general. the Fortinet FortiGate MIB includes the system information for the FortiGate and version of FortiOS. Both files are required for proper SNMP data collection.

To download the MIB files, go to **System > SNMP** and select a MIB link in the **FortiGate SNMP MIB** section.

Your SNMP manager may already include standard and private MIBs in a compiled database that is ready to use. You must add the Fortinet proprietary MIB to this database to have access to the Fortinet specific information.

There were major changes to the MIB files between FortiOS Carrier v3.0 and v4.0. You need to use the new MIBs for FortiOS Carrier v4.0 or you may mistakenly access the wrong traps and fields.

MIB files are updated for each version of FortiOS. When upgrading the firmware ensure that you updated the Fortinet FortiGate MIB file as well.

Fortinet MIBs

MIB file name or RFC	Description
FORTINET-CORE-MIB.mib	The Fortinet MIB includes all system configuration information and trap information that is common to all Fortinet products. Your SNMP manager requires this information to monitor FortiGate unit configuration settings and receive traps from the FortiGate SNMP agent.
FORTINET-FORTIGATE-MIB.mib	The FortiGate MIB includes all system configuration information and trap information that is specific to FortiGate units. Your SNMP manager requires this information to monitor FortiGate configuration settings and receive traps from the FortiGate SNMP agent. FortiManager systems require this MIB to monitor FortiGate units.

MIB file name or RFC	Description
RFC-1213 (MIB II)	The FortiGate SNMP agent supports MIB II groups with these exceptions. • No support for the EGP group from MIB II (RFC 1213, section 3.11 and 6.10). • Protocol statistics returned for MIB II groups (IP/ICMP/TCP/UDP/etc.) do not accurately capture all FortiGate traffic activity. More accurate information can be obtained from the information reported by the Fortinet MIB.
RFC-2665 (Ethernet-like MIB)	The FortiGate SNMP agent supports Ethernet-like MIB information. FortiGate SNMP does not support for the dot3Tests and dot3Errors groups.

SNMP improvements for dynamic routing include support for RFC 4750 OSPF Version 2 Management Information Base and RFC 5643 Management Information Base for OSPFv3. These changes add the capability of logging dynamic routing activity. Examples include sending OSPF routing events or changes to a syslog server or FortiAnalyzer or changes in neighborhood status.

Device detection for SNMP traps

This setting is related to the device detection feature. It allows SNMP traps to detect when a new device comes online. Within SNMP configurations there is a configurable timeout setting that periodically checks for the device. When a check determines that the device is present a trap is sent.

In the GUI, when configuring an SNMP object, one of the settings is a checkbox, under **SNMP Events** for **Device detected**.

To configure the SNMP object in the CLI use the following syntax:

```
config system snmp community
   edit <community ID number>
      set name <string>
      set events device-new
      end
```

In order to configure the idle timeout for the device, use the following syntax in the CLI:

```
config system global
   set device-idel-timeout <integer of time in seconds>
   end
```

The time value for the field can be set from 30 to 31536000.

SNMP get command syntax

Normally, to get configuration and status information for a FortiGate unit, an SNMP manager would use an SNMP get commands to get the information in a MIB field. The SNMP get command syntax would be similar to:

```
snmpget -v2c -c <community_name> <address_ipv4> {<OID> | <MIB_field>}
```

…where…

`<community_name>` is an SNMP community name added to the FortiGate configuration. You can add more than one community name to a FortiGate SNMP configuration. The most commonly used community name is `public`.

`<address_ipv4>` is the IP address of the FortiGate interface that the SNMP manager connects to.

`{<OID> | <MIB_field>}` is the object identifier (OID) for the MIB field or the MIB field name itself.

The SNMP `get` command gets firmware version running on the FortiGate unit. The community name is `public`. The IP address of the interface configured for SNMP management access is `10.10.10.1`. The firmware version MIB field is `fgSysVersion` and the OID for this MIB field is `1.3.6.1.4.1.12356.101.4.1.1` The first command uses the MIB field name and the second uses the OID:

```
snmpget -v2c -c public 10.10.10.1 fgSysVersion.0
snmpget -v2c -c public 10.10.10.1 1.3.6.1.4.1.12356.101.4.1.1.0
```

The OIDs and object names used in these examples are dependent on the version of MIB and are subject to change.

Replacement messages

The replacement message list in **System > Replacement Messages** enables you to view and customize replacement messages. Highlight the replacement messages you wish to edit and customize the message content to your requirements. Hit **Save** when done. If you do not see the message you want to edit, select the Extended View option (in the upper right-hand corner of the screen).

If you make a mistake, you can select the **Restore Default** to return to the original message and code base.

For connections requiring authentication, the FortiGate uses HTTP to send an authentication disclaimer page for the user to accept before a security policy is in effect. Therefore, you must initiate HTTP traffic first in order to trigger the authentication disclaimer page. Once the disclaimer is accepted, you can send whatever traffic is allowed by the security policy.

Replacement message images

You can add images to replacement messages to:

- Disclaimer pages
- Login pages
- Declined disclaimer pages
- Login failed page
- Login challenge pages
- Keepalive pages

Image embedding is also available to the endpoint NAC download portal and recommendation portal replacement messages, as well as HTTP replacement messages.

Supported image formats are GIF, JPEG, TIFF and PNG. The maximum file size supported is 24KB.

Adding images to replacement messages

To upload an image for use in a message

1. Go to **System > Replacement Messages**.
2. Select **Manage Images** at the top of the page.
3. Select **Create New**.
4. Enter a **Name** for the image.
5. Select the **Content Type**.
6. Select **Browse** to locate the file and select **OK**.

The image that you include in a replacement message, must have the following html:

```
<img src=%%IMAGE: <config_image_name>%% size=<bytes> >
```

For example:

```
<img src=%%IMAGE: logo_hq%% size=4272>
```

Modifying replacement messages

Replacement messages can be modified to include a message or content that suits your organization.

Use the expand arrows to view the replacement message list for a given category. Messages are in HTML format. To change a replacement message, go to **System > Replacement Messages** and select the replacement message that you want to modify. At the bottom pane of the window, you can see the message on one side and the HTML code on the other side. The message view changes in real-time as you change the content.

A list of common replacement messages appears in the main window. To see the entire list and all categories of replacement messages, in the upper-right corner of the window, select **Extended View**.

Replacement message categories

Alert email replacement messages

The FortiGate unit adds the replacement messages listed in this category to alert email messages sent to administrators. If you enable the option **Send alert email for logs based on severity** in **Log & Report**, you control whether or not replacement messages are sent by alert email based on how you set the **Minimum log level**.

For more information on Alert emails, see the Monitoring chapter.

Authentication replacement messages

The FortiGate unit uses the text of the authentication replacement messages for various user authentication HTML pages that are displayed when a user is required to authenticate because a security policy includes at least one identity-based policy that requires firewall users to authenticate.

These replacement message pages are for authentication using HTTP and HTTPS. You cannot customize the firewall authentication messages for FTP and Telnet.

The authentication login page and the authentication disclaimer include replacement tags and controls not found on other replacement messages.

Users see the authentication login page when they use a VPN or a security policy that requires authentication. You can customize this page in the same way as you modify other replacement messages.

There are some unique requirements for these replacement messages:

- The login page must be an HTML page containing a form with `ACTION="/"` and `METHOD="POST"`
- The form must contain the following hidden controls:
  - `<INPUT TYPE="hidden" NAME="%%MAGICID%%" VALUE="%%MAGICVAL%%">`
  - `<INPUT TYPE="hidden" NAME="%%STATEID%%" VALUE="%%STATEVAL%%">`
  - `<INPUT TYPE="hidden" NAME="%%REDIRID%%" VALUE="%%PROTURI%%">`
- The form must contain the following visible controls:
  - `<INPUT TYPE="text" NAME="%%USERNAMEID%%" size=25>`
  - `<INPUT TYPE="password" NAME="%%PASSWORDID%%" size=25>`

Example

The following is an example of a simple authentication page that meets the requirements listed above.

```
<HTML><HEAD><TITLE>Firewall Authentication</TITLE></HEAD>
      <BODY><H4>You must authenticate to use this service.</H4>
<FORM ACTION="/" method="post">
      <INPUT NAME="%%MAGICID%%" VALUE="%%MAGICVAL%%" TYPE="hidden">
<TABLE ALIGN="center" BGCOLOR="#00cccc" BORDER="0"
      CELLPADDING="15" CELLSPACING="0" WIDTH="320"><TBODY>
<TR><TH>Username:</TH>
      <TD><INPUT NAME="%%USERNAMEID%%" SIZE="25" TYPE="text"> </TD></TR>
<TR><TH>Password:</TH>
      <TD><INPUT NAME="%%PASSWORDID%%" SIZE="25" TYPE="password"> </TD></TR>
<TR><TD COLSPAN="2" ALIGN="center" BGCOLOR="#00cccc">
      <INPUT NAME="%%STATEID%%" VALUE="%%STATEVAL%%" TYPE="hidden">
          <INPUT NAME="%%REDIRID%%" VALUE="%%PROTURI%%" TYPE="hidden">
          <INPUT VALUE="Continue" TYPE="submit"> </TD></TR>
</TBODY></TABLE></FORM></BODY></HTML>
```

Captive Portal Default replacement messages

The Captive Portal Default replacement messages are used for wireless authentication only. You must have a VAP interface with the security set as captive portal to trigger these replacement messages.

Device Detection Portal replacement message

The FortiGate unit displays the replacement message when the FortiGate unit cannot determine the type of BYOD or handheld device is used to connect the network.

Email replacement messages

The FortiGate unit sends the mail replacement messages to email clients using IMAP, POP3, or SMTP when an event occurs such as antivirus blocking a file attached to an email that contains a virus. Email replacement messages are text messages.

If the FortiGate unit supports SSL content scanning and inspection these replacement messages can also be added to IMAPS, POP3S, and SMTPS email messages.

Endpoint Control replacement message

The FortiGate unit displays the replacement message when the FortiClient Endpoint Security software is not installed or registered correctly with the FortiGate unit.

FortiGuard Web Filtering replacement messages

The FortiGate unit sends the FortiGuard Web Filtering replacement messages to web browsers using the HTTP protocol when FortiGuard web filtering blocks a URL, provides details about blocked HTTP 4xx and 5xx errors, and for FortiGuard overrides. FortiGuard Web Filtering replacement messages are HTTP pages.

If the FortiGate unit supports SSL content scanning and inspection and if **Protocol Recognition > HTTPS Content Filtering Mode** is set to Deep Scan in the antivirus profile, these replacement messages can also replace web pages downloaded using the HTTPS protocol.

FTP replacement messages

The FortiGate unit sends the FTP replacement messages listed in the table below to FTP clients when an event occurs such as antivirus blocking a file that contains a virus in an FTP session. FTP replacement messages are text messages.

HTTP replacement messages

The FortiGate unit sends the HTTP replacement messages listed in the following table to web browsers using the HTTP protocol when an event occurs such as antivirus blocking a file that contains a virus in an HTTP session. HTTP replacement messages are HTML pages.

If the FortiGate unit supports SSL content scanning and inspection, and if under HTTPS in the protocol option list has Enable Deep Scan enabled, these replacement messages can also replace web pages downloaded using the HTTPS protocol.

NNTP replacement messages

The FortiGate unit sends the NNTP replacement messages NNTP clients when an event occurs such as antivirus blocking a file attached to an NNTP message that contains a virus. NNTP replacement messages are text messages.

Spam replacement messages

The FortiGate unit adds the Spam replacement messages to SMTP server responses if the email message is identified as spam and the spam action is discard. If the FortiGate unit supports SSL content scanning and inspection these replacement messages can also be added to SMTPS server responses.

NAC quarantine replacement messages

The page that is displayed for the user depends on whether NAC quarantine blocked the user because a virus was found, a DoS sensor detected an attack, an IPS sensor detected an attack, or a DLP rule with action set to **Quarantine IP address** or **Quarantine Interface** matched a session from the user.

The default messages inform the user of why they are seeing this page and recommend they contact the system administrator. You can customize the pages as required, for example to include an email address or other contact information or if applicable a note about how long the user can expect to be blocked.

SSL VPN replacement messages

The SSL VPN login replacement message is an HTML replacement message that formats the FortiGate SSL VPN portal login page. You can customize this replacement message according to your organization's needs. The page is linked to FortiGate functionality and you must construct it according to the following guidelines to ensure that it will work.

- The login page must be an HTML page containing a form with `ACTION="%%SSL_ACT%%"` and `METHOD="%%SSL_METHOD%%"`
- The form must contain the `%%SSL_LOGIN%%` tag to provide the login form.
- The form must contain the `%%SSL_HIDDEN%%` tag.

Web Proxy replacement messages

The FortiGate unit sends Web Proxy replacement messages when a web proxy event occurs that is detected and matches the web proxy configuration. These replacement messages are web pages that appear within your web browser.

The following web proxy replacement messages require an identity-based security policy so that the web proxy is successful. You can also enable FTP-over-HTTP by selecting the **FTP** option in **System > Network > Explicit Proxy**.

Traffic quota control replacement messages

When user traffic is going through the FortiGate unit and it is blocked by traffic shaping quota controls, users see the **Traffic shaper block message** or the **Per IP traffic shaper block message** when they attempt to connect through the FortiGate unit using HTTP.

The traffic quota HTTP pages should contain the `%%QUOTA_INFO%%` tag to display information about the traffic shaping quota setting that is blocking the user.

MM1 replacement messages

MM1 replacement messages are sent when, during MMS content scanning, FortiOS Carrier detects, for example a virus, using the MMS profile.

You must have **Remove Blocked** selected within the MMS profile if you want to remove the content that is intercepted during MMS scanning on the FortiGate unit.

MM3 replacement messages

MM3 replacement messages are sent when, during MMS content scanning, FortiOS Carrier detects, for example a virus, using the MMS profile.

You must have **Remove Blocked** selected within the MMS profile if you want to remove the content that is intercepted during MMS scanning on the unit.

MM4 replacement messages

MM4 replacement messages are sent when, during MMS content scanning, FortiOS Carrier detects, for example a virus, using the MMS profile.

MM7 replacement messages

MM7 replacement messages are sent when, during MMS content scanning, FortiOS Carrier detects, for example a virus, using the MMS profile.

MMS replacement messages

The MMS replacement message is sent when a section of an MMS message has been replaced because it contains a blocked file. This replacement message is in HTML format.

The message text is:

```
<HTML><BODY>This section of the message has been replaced because it contained a blocked
    file</BODY></HTML>
```

Replacement message groups

Replacement message groups enable you to view common messages in groups for large carriers. Message groups can be configured by going to **Config > Replacement Message Group**.

Using the defined groups, you can manage specific replacement messages from a single location, rather than searching through the entire replacement message list.

If you enable virtual domains (VDOMs) on the FortiGate unit, replacement message groups are configured separately for each virtual domain. Each virtual domain has its own default replacement message group, configured from **System > Replacement Messages Group**.

When you modify a message in a replacement message group, a Reset icon appears beside the message in the group. You can select this Reset icon to reset the message in the replacement message group to the default version.

All MM1/4/7 notification messages for FortiOS Carrier (and MM1 retrieve-conf messages) can contain a SMIL layer and all MM4 notification messages can contain an HTML layer in the message. These layers can be used to brand messages by using logos uploaded to the FortiGate unit via the 'Manage Images' link found on the replacement message group configuration page.

Administration for schools

For a system administrator in a school system, it is difficult to maintain a network and access to the Internet. There are potential legal liabilities if content is not properly filtered and students gain access to pornography and other non-productive and potentially dangerous content. This section describes some basic practices administrators can employ.

Security policies

The default security policies in FortiOS allow all traffic on all ports and all IP addresses. While applying security profiles can help to block viruses, detect attacks and prevent spam, this doesn't provide a solid overall security option. The best approach is a layered approach; the first layer being the security policy.

When creating outbound security policies, you need to identify what the students are allowed to do. Generally, they surf the web, connect to FTP sites, send and receive email, and so on.

Once you know what the students need to do, you can research the software used and determine the ports the applications use. For example, if the students only require web surfing, then there are only two ports (80 - HTTP and 443 - HTTPS) needed to complete their tasks. Setting the security policies to only allow traffic through two ports (rather than all 65,000), this will significantly lower any possible exploits. By restricting the ports to known services, means stopping the use of proxy servers, as many of them operate on a non-standard port to hide their traffic from URL filtering or HTTP inspection.

DNS

You should restrict the students use of DNS. We recommend that you point to an internal DNS server and only allow those devices out on port 53.

If there is no internal DNS server, then you should establish a restrictive list of allowed DNS servers students can use. One possible exploit would be for them to set up their own DNS server at home that serves different IPs for known hosts, such as having Google.com sent back the IP for playboy.com.

Encrypted traffic (HTTPS)

Generally speaking, students should not be allowed to access encrypted web sites. Encrypted traffic can't be sniffed, and therefore, can't be monitored. HTTPS traffic should only be allowed when necessary. Most web sites a student needs to access are HTTP, not HTTPS. Due to the nature of HTTPS protocol, and the fact that encryption is an inherent security risk to your network, its use should be restricted.

To ensure that students only visit HTTPS sites required for schoolwork, we recommend that you add a security policy that designates a list of allowed secure sites.

FTP

For the most part, students should not be using FTP. FTP is not HTTP or HTTPS so you can't use URL filtering to restrict where they go. This can be controlled with destination IPs in the security policy. With a policy that specifically outlines which FTP addresses are allowed, all other will be blocked.

Example security policies

Given these recommended practices, a set of security policies could look like the following illustration. In a large setup, all the IPs for the students are treated by one of these four policies.

Simple security policy setup

ID	Name	From	To	Source	Destination	Schedule	Service	Action	Status
2	restrict https	internal	wan1	all Students	Allowed Websites	always	HTTPS	ACCEPT	Enabled
3	all http	internal	wan1	all Students	all	always	HTTP	ACCEPT	Enabled
4	allowed dns	internal	wan1	all Students	Allowed DNS	always	DNS	ACCEPT	Enabled
5	allowed ftp	internal	wan1	all Students	Allowed FTP	always	FTP	ACCEPT	Enabled
0	Implicit Deny	any	any	all	all	always	ALL	DENY	

The last policy in the list is the deny policy that is configured by default. The deny policy ensures that any traffic making it to this point is stopped. It can also help in further troubleshooting by viewing the logs for denied traffic.

With these policies in place, even before packet inspection occurs, the FortiGate, and the network are fairly secure. Should any of the UTM profiles fail, there is still a basic level of security.

Security profiles

AntiVirus profiles

You should enable antivirus screening for any service that is enabled in the security policies. In the case above, HTTP, FTP, as well as POP3 and SMTP (assuming there is email access for students). There is not a virus scan option for HTTPS, because the content is encrypted. Generally speaking, most of the network traffic will be students surfing the web.

To configure antivirus profiles in the GUI, go to Security Profiles > AntiVirus.

Web filtering

We recommend that you configure your FortiGate to filter URLs, sites and content, using FortiGuard web filtering service. Web sites are constantly being monitored, and new ones reviewed and added to the FortiGuard databases every day. The FortiGuard categories provide an extensive list of offensive and non-productive sites.

There are additional settings to include in a web filtering profile to best contain a student's web browsing. You can enable safe search, restrict YouTube access, block invalid URLs, and block malicious URLs discovered by FortiSandbox. For more information on these options, see the web filtering section in the Security Profiles chapter.

To configure web filtering options, go to **Security Profiles > Web Filter**.

Categories and classifications

The selection of what FortiGuard categories and classifications that should be blocked is based on the school system and its Internet information policy.

Email filtering

Other than specific teacher-led email inboxes, there is no reason why a student should be able to access, read or send personal email. Ports for POP3, SMTP and IMAP should not be opened in a security policy.

IPS

The intrusion prevention profiles are used to ensure the student PCs are not vulnerable to attacks and are not in a position to make attacks. As well, IPS can do more than simple vulnerability scans. With a FortiGuard subscription, IPS signatures are pushed to the FortiGate unit. New signatures are released regularly for intrusions as they are discovered.

FortiOS includes a number of predefined IPS sensors that you can enable by default. To configure IPS sensors, go to **Security Profiles > Intrusion Prevention**.

Application control

Application control uses IPS signatures to limit the use of instant messaging and peer-to-peer applications which can lead to possible infections on a student's PC. FortiOS includes a number of pre-defined application categories. To configure and maintain application control profiles, go to **Security Profiles > Application Control**.

Some applications to consider include proxies, botnets, toolbars and P2P applications.

Logging

Turn on all logging. Every option in this section should be enabled. This is not where you decide what you are going to log. You are identifying what the profiles can log.

Logging everything is a way to monitor traffic on the network, see what student's are utilizing the most, and locate any potential holes in your security plan. Keeping this information may help to prove negligence later if necessary.

PPTP and L2TP

A virtual private network (VPN) is a way to use a public network, such as the Internet, as a vehicle to provide remote offices or individual users with secure access to private networks. FortiOS supports the Point-to-Point Tunneling Protocol (PPTP), which enables interoperability between FortiGate units and Windows or Linux PPTP clients. Because FortiGate units support industry standard PPTP VPN technologies, you can configure a PPTP VPN between a FortiGate unit and most third-party PPTP VPN peers.

This section describes how to configure PPTP and L2TP VPNs as well as PPTP passthrough.

This section includes the topics:

How PPTP VPNs work

The Point-to-Point Tunneling Protocol enables you to create a VPN between a remote client and your internal network. Because it is a Microsoft Windows standard, PPTP does not require third-party software on the client computer. As long as the ISP supports PPTP on its servers, you can create a secure connection by making relatively simple configuration changes to the client computer and the FortiGate unit.

PPTP uses Point-to-Point protocol (PPP) authentication protocols so that standard PPP software can operate on tunneled PPP links. PPTP packages data in PPP packets and then encapsulates the PPP packets within IP packets for transmission through a VPN tunnel.

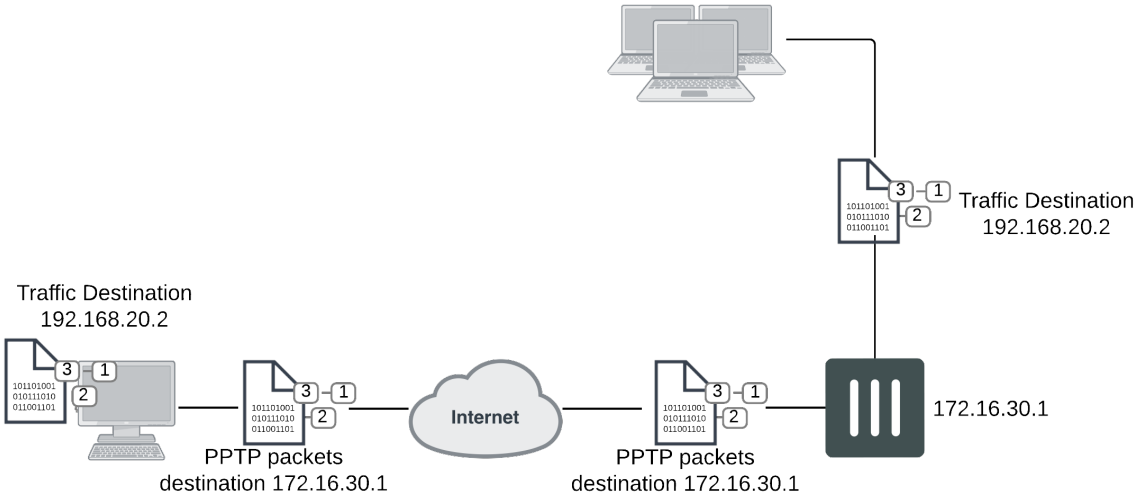
When the FortiGate unit acts as a PPTP server, a PPTP session and tunnel is created as soon as the PPTP client connects to the FortiGate unit. More than one PPTP session can be supported on the same tunnel. FortiGate units support PAP, CHAP, and plain text authentication. PPTP clients are authenticated as members of a user group.

Traffic from one PPTP peer is encrypted using PPP before it is encapsulated using Generic Routing Encapsulation (GRE) and routed to the other PPTP peer through an ISP network. PPP packets from the remote client are addressed to a computer on the private network behind the FortiGate unit. PPTP packets from the remote client are addressed to the public interface of the FortiGate unit. Seethe figure below.

PPTP control channel messages are not authenticated, and their integrity is not protected. Furthermore, encapsulated PPP packets are not cryptographically protected and may be read or modified unless appropriate encryption software such as Secure Shell (SSH) or Secure File Transfer Protocol (SFTP) is used to transfer data after the tunnel has been established.

As an alternative, you can use encryption software such as Microsoft Point-to-Point Encryption (MPPE) to secure the channel. MPPE is built into Microsoft Windows clients and can be installed on Linux clients. FortiGate units support MPPE.

Packet encapsulation



Shown above, traffic from the remote client is addressed to a computer on the network behind the FortiGate unit. When the PPTP tunnel is established, packets from the remote client are encapsulated and addressed to the FortiGate unit. The FortiGate unit forwards disassembled packets to the computer on the internal network.

When the remote PPTP client connects, the FortiGate unit assigns an IP address from a reserved range of IP addresses to the client PPTP interface. The PPTP client uses the assigned IP address as its source address for the duration of the connection.

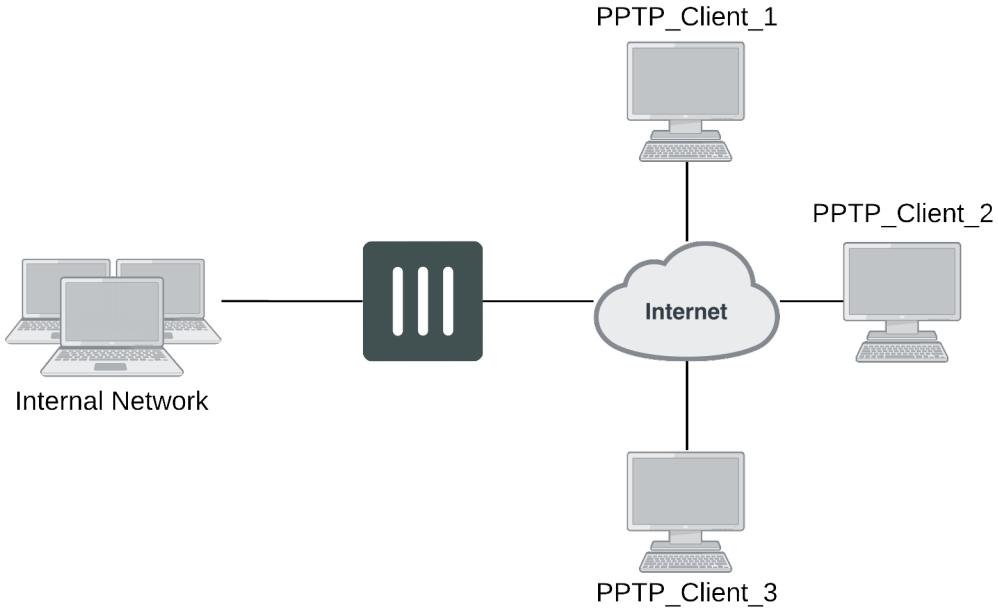
When the FortiGate unit receives a PPTP packet, the unit disassembles the PPTP packet and forwards the packet to the correct computer on the internal network. The security policy and protection profiles on the FortiGate unit ensure that inbound traffic is screened and processed securely.

PPTP clients must be authenticated before a tunnel is established. The authentication process relies on FortiGate user group definitions, which can optionally use established authentication mechanisms such as RADIUS or LDAP to authenticate PPTP clients. All PPTP clients are challenged when a connection attempt is made.

FortiGate unit as a PPTP server

In the most common Internet scenario, the PPTP client connects to an ISP that offers PPP connections with dynamically-assigned IP addresses. The ISP forwards PPTP packets to the Internet, where they are routed to the FortiGate unit.

FortiGate unit as a PPTP server



If the FortiGate unit will act as a PPTP server, there are a number of steps to complete:

- Configure user authentication for PPTP clients.
- Enable PPTP.
- Specify the range of addresses that are assigned to PPTP clients when connecting
- Configure the security policy.

Configuring user authentication for PPTP clients

To enable authentication for PPTP clients, you must create user accounts and a user group to identify the PPTP clients that need access to the network behind the FortiGate unit. Within the user group, you must add a user for each PPTP client.

You can choose to use a plain text password for authentication or forward authentication requests to an external RADIUS, LDAP, or TACACS+ server. If password protection will be provided through a RADIUS, LDAP, or TACACS+ server, you must configure the FortiGate unit to forward authentication requests to the authentication server.

This example creates a basic user/password combination.

Configuring a user account

To add a local user - GUI

1. Go to **User & Device > User Definition** and select **Create New.**
2. Select **Local User**
3. Enter a **User Name**.
4. Enter a **Password** for the user. The password should be at least six characters.
5. Select **OK**.

To add a local user - CLI

```
config user local
   edit <username>
      set type password
      set passwd <password>
end
```

Configuring a user group

To ease configuration, create user groups that contain users in similar categories or departments.

To create a user group - GUI

1. Go to **User & Device > User Group** and select **Create New**.
2. Enter a **Name** for the group.
3. Select the **Type** of **Firewall**.
4. From the **Available Users** list, select the required users and select the right-facing arrow to add them to the **Members** list.
5. Select **OK**.

To create a user group - CLI

```
config user group
   edit <group_name>
      set group-type firewall
      set member <user_names>
end
```

Enabling PPTP and specifying the PPTP IP address range

The PPTP address range specifies the range of addresses reserved for remote PPTP clients. When a PPTP client connects to the FortiGate unit, the client is assigned an IP address from this range. Afterward, the FortiGate unit uses the assigned address to communicate with the PPTP client.

The address range that you reserve can be associated with private or routable IP addresses. If you specify a private address range that matches a network behind the FortiGate unit, the assigned address will make the PPTP client appear to be part of the internal network.

PPTP requires two IP addresses, one for each end of the tunnel. The PPTP address range is the range of addresses reserved for remote PPTP clients. When the remote PPTP client establishes a connection, the FortiGate unit assigns an IP address from the reserved range of IP addresses to the client PPTP interface or retrieves the assigned IP address from the PPTP user group. If you use the PPTP user group, you must also define the FortiGate end of the tunnel by entering the IP address of the unit in **Local IP** (web-based manager) ***or*** `local-ip` (CLI). The PPTP client uses the assigned IP address as its source address for the duration of the connection.

PPTP configuration is only available through the CLI. In the example below, PPTP is enabled with the use of an IP range of `192.168.1.1` to `192.168.1.10` for addressing and the user group is hr_staff.

FortiOS 5.4.0 and later versions allow the start and end IPs in the PPTP address range to be in the same 16-bit subnet. Earlier versions require that the start and end IPs in the PPTP address range be in the same 24-bit subnet, for example, 192.168.1.1 - 192.168.1.254. .

```
config vpn pptp
   set status enable
   set ip-mode range
   set eip 192.168.1.10
   set sip 192.168.1.1
   set usrgrp hr_staff
end
```

In this example, PPTP is enabled with the use of a user group for addressing, where the IP address of the PPTP server is `192.168.1.2` and the user group is `hr_admin`.

```
config vpn pptp
   set status enable
   set ip-mode range
   set local-ip 192.168.2.1
   set usrgrp hr_admin
end
```

Adding the security policy

The security policy specifies the source and destination addresses that can generate traffic inside the PPTP tunnel and defines the scope of services permitted through the tunnel. If a selection of services are required, define a service group.

To configure the firewall for the PPTP tunnel - GUI

1. Go to **Policy & Objects > IPv4** or **Policy & Objects > IPv6** and select **Create New**.
2. Complete the following and select **OK**:

Incoming Interface	The FortiGate interface connected to the Internet.
Source Address	Select the name that corresponds to the range of addresses that you reserved for PPTP clients.
Outgoing Interface	The FortiGate interface connected to the internal network.

Destination Address	Select the name that corresponds to the IP addresses behind the FortiGate unit.
Schedule	always
Service	ALL
Action	ACCEPT

To configure the firewall for the PPTP tunnel - CLI

```
config firewall policy or config firewall policy6
   edit 1
      set srcintf <interface to internet>
      set dstintf <interface to internal network>
      set srcaddr <reserved_range>
      set dstaddr <internal_addresses>
      set action accept
      set schedule always
      set service ALL
end
```

Configuring the FortiGate unit for PPTP VPN

To arrange for PPTP packets to pass through the FortiGate unit to an external PPTP server, perform the following tasks in the order given:

- Configure user authentication for PPTP clients.
- Enable PPTP on the FortiGate unit and specify the range of addresses that can be assigned to PPTP clients when they connect.
- Configure PPTP pass through on the FortiGate unit.

Configuring the FortiGate unit for PPTP passthrough

To forward PPTP packets to a PPTP server on the network behind the FortiGate unit, you need to perform the following configuration tasks on the FortiGate unit:

- Define a virtual IP address that points to the PPTP server.
- Create a security policy that allows incoming PPTP packets to pass through to the PPTP server.

The address range is the external (public) ip address range which requires access to the internal PPTP server through the FortiGate virtual port-forwarding firewall.

IP addresses used in this document are fictional and follow the technical documentation guidelines specific to Fortinet. Real external IP addresses are not used.

Configuring a virtual IP address

The virtual IP address will be the address of the PPTP server host.

To define a virtual IP for PPTP passthrough - GUI

1. Go to **Policy & Objects > Virtual IPs**.
2. Select **Create New**.
3. Choose the **VIP Type**.
4. Enter the name of the VIP, for example, `PPTP_Server`.
5. Select the **External Interface** where the packets will be received for the PPTP server.
6. Enter the **External IP Address** for the VIP.
7. Select **Port Forwarding**.
8. Set the **Protocol to TCP**.
9. Enter the **External Service Port** of `1723`, the default for PPTP.
10. Enter the **Map to Port** to `1723`.
11. Select **OK**.

To define a virtual IP for PPTP passthrough - CLI

```
config firewall vip or config firewall vip6
   edit PPTP_Server
      set extintf <interface>
      set extip <ip_address>
      set portforward enable
      set protocol tcp
      set extport 1723
      set mappedport 1723
      set mappedip <destination IP address range>
      end
```

You can also use `config firewall vip46` to define a virtual IP from an IPv4 address to an IPv6 address or `config firewall vip64` to define a virtual IP from an IPv6 address to an IPv4 address.

Configuring a port-forwarding security policy

To create a port-forwarding security policy for PPTP passthrough you must first create an address range reserved for the PPTP clients.

To create an address range - GUI

1. Go to **Policy & Objects > Addresses** and select **Create New**.
2. Select a **Category**.
3. Enter a **Name** for the range, for example, `External_PPTP`.
4. Select a **Type** of **Subnet/IP Range**.
5. Enter the IP address range.
6. Select the **Interface** to the Internet.
7. Select **OK**.

To create an address range - CLI

```
config firewall address OR config firewall address6
   edit External_PPTP
      set type ip_range
      set start-ip <ip_address>
      set end-ip <ip_address>
      set associated-interface <internet_interface>
end
```

With the address set, you can add the security policy.

To add the security policy - GUI

1. Go to **Policy & Objects > IPv4** or **Policy & Objects > IPv6** and select **Create New**.
2. Complete the following and select **OK**:

Incoming Interface	The FortiGate interface connected to the Internet.
Source Address	Select the address range created in the previous step.
Outgoing Interface	The FortiGate interface connected to the PPTP server.
Destination Address	Select the VIP address created in the previous steps.
Schedule	always
Service	PPTP
Action	ACCEPT

To add the security policy - CLI

```
config firewall policy or config firewall policy6
   edit <policy_number>
      set srcintf <interface to internet>
      set dstintf <interface to PPTP server>
      set srcaddr <address_range>
      set dstaddr <PPTP_server_address>
      set action accept
      set schedule always
      set service PPTP
end
```

Testing PPTP VPN connections

To confirm that a PPTP VPN between a local network and a dialup client has been configured correctly, at the dialup client, issue a ping command to test the connection to the local network. The PPTP VPN tunnel initializes when the dialup client attempts to connect.

Logging VPN events

PPTP VPN, activity is logged when enabling VPN logging. The FortiGate unit connection events and tunnel status (up/down) are logged.

To log VPN events

1. Go to **Log & Report > Log Settings**.
2. Enable **Event Logging**.
3. Select **VPN activity event**.
4. Select **Apply**.

To view event logs

1. Go to **Log & Report > VPN Events**.
2. If the option is available to set the log location list, select disk or memory.
3. Select a log event and select **Details**.

Configuring L2TP VPNs

This section describes how to configure a FortiGate unit to establish a Layer Two Tunneling Protocol (L2TP) tunnel with a remote dialup client. The FortiGate implementation of L2TP enables a remote dialup client to establish an L2TP tunnel with the FortiGate unit directly.

According to RFC 2661, an Access Concentrator (LAC) can establish an L2TP tunnel with an L2TP Network Server (LNS). In a typical scenario, the LAC is managed by an ISP and located on the ISP premises; the LNS is the gateway to a private network. When a remote dialup client connects to the Internet through the ISP, the ISP uses a local database to establish the identity of the caller and determine whether the caller needs access to an LNS through an L2TP tunnel. If the services registered to the caller indicate that an L2TP connection to the LNS is required, the ISP LAC attempts to establish an L2TP tunnel with the LNS.

A FortiGate unit can be configured to act as an LNS. The FortiGate implementation of L2TP enables a remote dialup client to establish an L2TP tunnel with the FortiGate unit directly, bypassing any LAC managed by an ISP. The ISP must configure its network access server to forward L2TP traffic from the remote client to the FortiGate unit directly whenever the remote client requires an L2TP connection to the FortiGate unit.

When the FortiGate unit acts as an LNS, an L2TP session and tunnel is created as soon as the remote client connects to the FortiGate unit. The FortiGate unit assigns an IP address to the client from a reserved range of IP addresses. The remote client uses the assigned IP address as its source address for the duration of the connection.

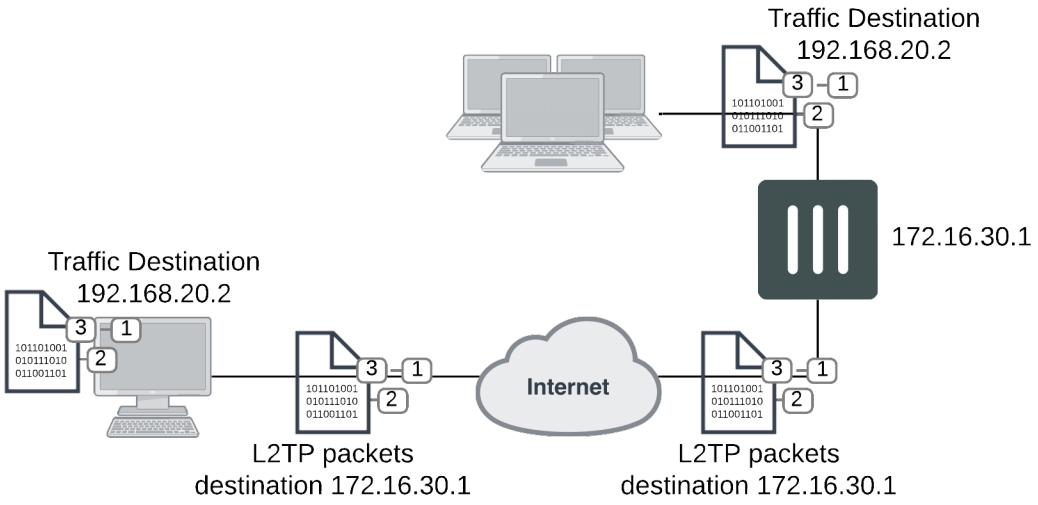
More than one L2TP session can be supported on the same tunnel. FortiGate units can be configured to authenticate remote clients using a plain text user name and password, or authentication can be forwarded to an external RADIUS or LDAP server. L2TP clients are authenticated as members of a user group.

For site-to-site connections, Windows servers use IPsec encryption when you configure the VPN to connect to an L2TP server.

Traffic from the remote client must be encrypted using IPsec before it is encapsulated and routed to the FortiGate unit. Packets originating at the remote client are addressed to a computer on the private network behind the FortiGate unit. Encapsulated packets are addressed to the public interface of the FortiGate unit. See the figure below.

When the FortiGate unit receives an L2TP packet, the unit disassembles the packet and forwards the packet to the correct computer on the internal network. The security policy and protection profiles on the FortiGate unit ensure that inbound traffic is screened and processed securely.

L2TP encapsulation

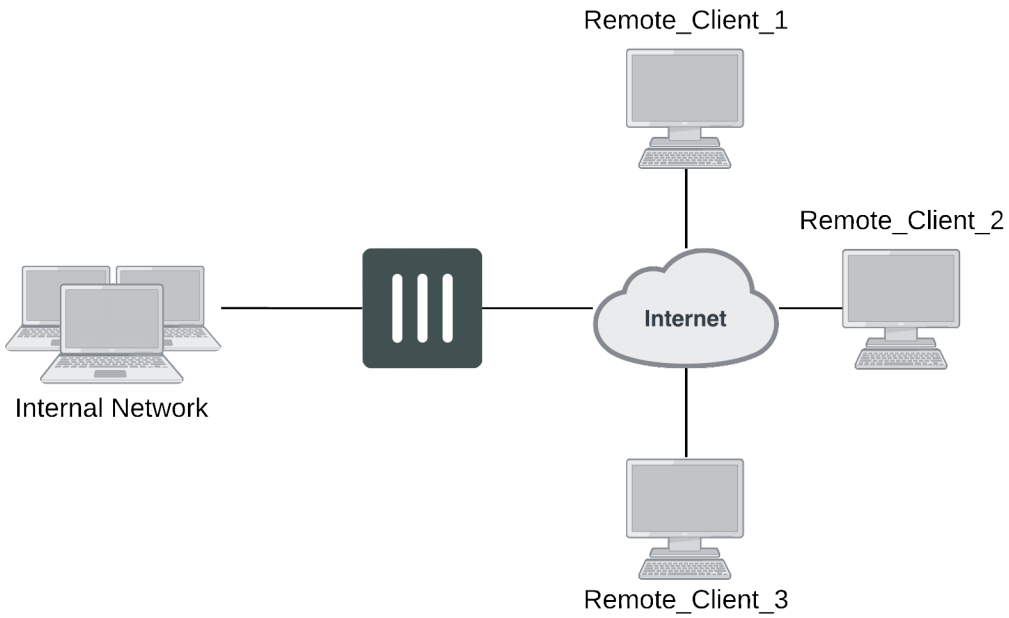


FortiGate units cannot deliver non-IP traffic such as Frame Relay or ATM frames encapsulated in L2TP packets — FortiGate units support the IPv4 and IPv6 addressing schemes only

Network topology

The remote client connects to an ISP that determines whether the client requires an L2TP connection to the FortiGate unit. If an L2TP connection is required, the connection request is forwarded to the FortiGate unit directly.

Example L2TP configuration



L2TP infrastructure requirements

- The FortiGate unit must be operating in NAT mode and have a static public IP address.
- The ISP must configure its network access server to forward L2TP traffic from remote clients to the FortiGate unit directly.
- The remote client must not generate non-IP traffic (Frame Relay or ATM frames).

L2TP configuration overview

To configure a FortiGate unit to act as an LNS, you perform the following tasks:

- Create an L2TP user group containing one user for each remote client.
- Enable L2TP on the FortiGate unit and specify the range of addresses that can be assigned to remote clients when they connect.
- Define firewall source and destination addresses to indicate where packets transported through the L2TP tunnel will originate and be delivered.
- Create the security policy and define the scope of permitted services between the source and destination addresses.
- Configure the remote clients.

Authenticating L2TP clients

L2TP clients must be authenticated before a tunnel is established. The authentication process relies on FortiGate user group definitions, which can optionally use established authentication mechanisms such as RADIUS or LDAP to authenticate L2TP clients. All L2TP clients are challenged when a connection attempt is made.

To enable authentication, you must create user accounts and a user group to identify the L2TP clients that need access to the network behind the FortiGate unit.

You can choose to use a plain text password for authentication or forward authentication requests to an external RADIUS or LDAP server. If password protection will be provided through a RADIUS or LDAP server, you must configure the FortiGate unit to forward authentication requests to the authentication server.

Enabling L2TP and specifying an address range

The L2TP address range specifies the range of addresses reserved for remote clients. When a remote client connects to the FortiGate unit, the client is assigned an IP address from this range. Afterward, the FortiGate unit uses the assigned address to communicate with the remote client.

The address range that you reserve can be associated with private or routable IP addresses. If you specify a private address range that matches a network behind the FortiGate unit, the assigned address will make the remote client appear to be part of the internal network.

To enable L2TP and specify the L2TP address range, use the `config vpn l2tp` CLI command.

The following example shows how to enable L2TP and set the L2TP address range using a starting address of `192.168.10.80` and an ending address of `192.168.10.100` for an existing group of L2TP users named `L2TP_users`:

```
config vpn l2tp
   set sip 192.168.10.80
   set eip 192.168.10.100
   set status enable
   set usrgrp L2TP_users
end
```

Defining firewall source and destination addresses

Before you define the security policy, you must define the source and destination addresses of packets that are to be transported through the L2TP tunnel:

- For the source address, enter the range of addresses that you reserved for remote L2TP clients (for example `192.168.10.[80-100]`).
- For the destination address, enter the IP addresses of the computers that the L2TP clients need to access on the private network behind the FortiGate unit (for example, `172.16.5.0/24` for a subnet, or `172.16.5.1` for a server or host, or `192.168.10.[10-15]` for an IP address range).

To define the firewall source address

1. Go to **Policy & Objects > Addresses** and select **Create New**.
2. Select **Address**.
3. In the **Name** field, type a name that represents the range of addresses that you reserved for remote clients (for example, `Ext_L2TPrange`).

4. In **Type**, select **IP Range**.
5. In the **Subnet / IP Range** field, type the corresponding IP address range.
6. In **Interface**, select the FortiGate interface that connects to the clients.
7. This is usually the interface that connects to the Internet.
8. Select **OK**.

To define the firewall destination address

1. Go to **Policy & Objects > Addresses** and select **Create New**.
2. In the **Address Name** field, type a name that represents a range of IP addresses on the network behind the FortiGate unit (for example, `Int_L2TPaccess`).
3. In **Type**, select **IP Range**.
4. In the **IP Range** field, type the corresponding IP address range.
5. In **Interface**, select the FortiGate interface that connects to the network behind the FortiGate unit.
6. Select **OK**.

Adding the security policy

The security policy specifies the source and destination addresses that can generate traffic inside the L2TP tunnel and defines the scope of services permitted through the tunnel. If a selection of services are required, define a service group.

To define the traffic and services permitted inside the L2TP tunnel

1. Go to **Policy & Objects > IPv4** or **Policy & Objects > IPv6** and select **Create New**.
2. Enter these settings:

Name	Input a name for the policy.
Incoming Interface	Select the FortiGate interface to the Internet.
Outgoing Interface	Select the FortiGate interface to the internal (private) network.
Source Address	Select the name that corresponds to the address range that reserved for L2TP clients (for example, `Ext_L2TPrange`).
Destination Address	Select the name that corresponds to the IP addresses behind the FortiGate unit (for example, `Int_L2TPaccess`).
Schedule	Select ALWAYS, or if a select schedule is required instead, select a schedule that you defined previously.
Service	Select ALL, or if selected services are required instead, select the service group that you defined previously.
Action	ACCEPT

3. Select **OK**.

Configuring a Linux client

This procedure outlines how to install L2TP client software and run an L2TP tunnel on a Linux computer. Obtain an L2TP client package that meets your requirements (for example, `rp-l2tp`). If needed to encrypt traffic, obtain L2TP client software that supports encryption using IPsec.

To establish an L2TP tunnel with a FortiGate unit that has been set up to accept L2TP connections, you can obtain and install the client software following these guidelines:

1. If encryption is required, you will need to verify the IPsec configuration.
2. Download and install the L2TP client package.
3. Configure an L2TP connection to run the L2TP program.
4. Configure routes to determine whether all or some of your network traffic will be sent through the tunnel. You must define a route to the remote network over the L2TP link and a host route to the FortiGate unit.
5. Run `l2tpd` to start the tunnel.

Follow the software supplier's documentation to complete the steps.

To configure the system, you need to know the public IP address of the FortiGate unit, and the user name and password that has been set up on the FortiGate unit to authenticate L2TP clients. Contact the FortiGate administrator if required to obtain this information.

Monitoring L2TP sessions

You can display a list of all active sessions and view activity by port number. By default, port 1701 is used for L2TP VPN-related communications. If required, active sessions can be stopped from this view. Use **FortiView > All Sessions**.

Testing L2TP VPN connections

To confirm that a VPN between a local network and a dialup client has been configured correctly, at the dialup client, issue a ping command to test the connection to the local network. The VPN tunnel initializes when the dialup client attempts to connect.

Logging L2TP VPN events

You can configure the FortiGate unit to log VPN events. For L2TP VPNs, connection events and tunnel status (up/down) are logged.

To log VPN events - GUI

1. Go to **Log & Report > Log Settings**.
2. Enable the storage of log messages to one or more locations.
3. Select **Enable**, and then select **VPN activity event**.
4. Select **Apply**.

To log VPN events - CLI

```
config log memory setting
   set diskfull overwrite
   set status enable
```

```
end
config log eventfilter
   set vpn enable
end
```

Session helpers

FortiOS uses session helpers to process sessions that have special requirements. Session helpers function like proxies by getting information from the session and performing support functions required by the session. For example:

The SIP session helper looks inside SIP messages and performs NAT (if required) on the IP addresses in the SIP message and opens pinholes to allow media traffic associated with the SIP session to pass through the FortiGate unit.

The FTP session helper can keep track of multiple connections initiated from a single FTP session. The session helper also permits an FTP server to actively open a connection back to a client program.

The TNS session helper sniffs the return packet from an initial 1521 SQLNET exchange and then uses the port and session information uncovered in that return TNS redirect packet to add a temporary firewall policy that accepts the new port and IP address supplied as part of the TNS redirect.

The session helper configuration binds a session helper to a TCP or UDP port and protocol. When a session is accepted by a firewall policy on that port and protocol the FortiOS passes the session to the session helper configured with this command. The session is processed by the session helper.

If your FortiGate accepts sessions that require a session helper on different ports than those defined by the session-helper configuration, then you can add more entries to the session helper configuration. Its OK to have multiple session helper configurations for a given protocol because only the matching configuration is used.

Use the show system session-helper command to view the current session helper configuration.

This section includes the topics:

Viewing the session helper configuration

You can view the session helpers enabled on your FortiGate unit in the CLI using the commands below. The following output shows the first two session helpers. The number of session helpers can vary to around 20.

```
show system session-helper
   config system session-helper
      edit 1
         set name pptp
         set port 1723
         set protocol 6
      next
         set name h323
         set port 1720
         set protocol 6
      end
      .
      .
```

The configuration for each session helper includes the name of the session helper and the port and protocol number on which the session helper listens for sessions. Session helpers listed on protocol number 6 (TCP) or 17 (UDP). For a complete list of protocol numbers see Assigned Internet Protocol Numbers.

For example, the output above shows that FortiOS listens for PPTP packets on TCP port 1723 and H.323 packets on port TCP port 1720.

If a session helper listens on more than one port or protocol the more than one entry for the session helper appears in the `config system session-helper` list. For example, the pmap session helper appears twice because it listens on TCP port 111 and UDP port 111. The rsh session helper appears twice because it listens on TCP ports 514 and 512.

Changing the session helper configuration

Normally you will not need to change the configuration of the session helpers. However in some cases you may need to change the protocol or port the session helper listens on.

Changing the protocol or port that a session helper listens on

Most session helpers are configured to listen for their sessions on the port and protocol that they typically use. If your FortiGate unit receives sessions that should be handled by a session helper on a non-standard port or protocol you can use the following procedure to change the port and protocol used by a session helper. The following example shows how to change the port that the pmap session helper listens on for Sun RPC portmapper TCP sessions. By default pmap listens on TCP port 111.

To change the port that the pmap session helper listens on to TCP port 112

1. Confirm that the TCP pmap session helper entry is 11 in the session-helper list:

```
show system session-helper 11
   config system session-helper
      edit 11
```

```
            set name pmap
            set port 111
            set protocol 6
        next
    end
```

2. Enter the following command to change the TCP port to 112.

```
config system session-helper
    edit 11
        set port 112
    end
```

3. The pmap session helper also listens on UDP port 111. Confirm that the UDP pmap session helper entry is 12 in the session-helper list:

```
show system session-helper 12
    config system session-helper
        edit 12
            set name pmap
            set port 111
            set protocol 17
        next
    end
```

4. Enter the following command to change the UDP port to 112.

```
config system session-helper
    edit 12
        set port 112
        end
```

Use the following command to set the h323 session helper to listen for ports on the UDP protocol.

To change the protocol that the h323 session helper listens on

1. Confirm that the h323 session helper entry is 2 in the session-helper list:

```
show system session-helper 2
    config system session-helper
        edit 2
            set name h323
            set port 1720
            set protocol 6
        next
    end
```

2. Enter the following command to change the protocol to UDP.

```
config system session-helper
    edit 2
        set protocol 17
        end
```

If a session helper listens on more than one port or protocol, then multiple entries for the session helper must be added to the session helper list, one for each port and protocol combination. For example, the rtsp session helper listens on TCP ports 554, 7070, and 8554 so there are three rtsp entries in the session-helper list. If your FortiGate unit receives rtsp packets on a different TCP port (for example, 6677) you can use the following command to configure the rtsp session helper to listen on TCP port 6677.

To configure a session helper to listen on a new port and protocol

```
config system session-helper
   edit 0
      set name rtsp
      set port 6677
      set protocol 6
      end
```

Disabling a session helper

In some cases you may need to disable a session helper. Disabling a session helper just means removing it from the session-helper list so that the session helper is not listening on a port. You can completely disable a session helper by deleting all of its entries from the session helper list. If there are multiple entries for a session helper on the list you can delete one of the entries to prevent the session helper from listening on that port.

To disable the mgcp session helper from listening on UDP port 2427

1. Enter the following command to find the mgcp session helper entry that listens on UDP port 2427:

```
show system session-helper
   .
   .
   .
edit 19
   set name mgcp
   set port 2427
   set protocol 17
next
   .
   .
   .
```

2. Enter the following command to delete session-helper list entry number 19 to disable the mgcp session helper from listening on UDP port 2427:

```
config system session-helper
   delete 19
```

By default the mgcp session helper listens on UDP ports 2427 and 2727. The previous procedure shows how to disable the mgcp protocol from listening on port 2427. The following procedure completely disables the mgcp session helper by also disabling it from listening on UDP port 2727.

To completely disable the mgcp session helper

1. Enter the following command to find the mgcp session helper entry that listens on UDP port 2727:

```
show system session-helper
   .
   .
   .
edit 20
   set name mgcp
   set port 2727
   set protocol 17
next
   .
   .
   .
```

2. Enter the following command to delete session-helper list entry number 20 to disable the mgcp session helper from listening on UDP port 2727:

```
config system session-helper
   delete 20
```

DCE-RPC session helper (dcerpc)

Distributed Computing Environment Remote Procedure Call (DCE-RPC) provides a way for a program running on one host to call procedures in a program running on another host. DCE-RPC (also called MS RPC for Microsoft RPC) is similar to ONC-RPC. Because of the large number of RPC services, for example, MAPI, the transport address of an RPC service is dynamically negotiated based on the service program's universal unique identifier (UUID). The Endpoint Mapper (EPM) binding protocol in FortiOS maps the specific UUID to a transport address.

To accept DCE-RPC sessions you must add a security policy with service set to **ALL** or to the DEC-RPC pre-defined service (which listens on TCP and UDP ports 135). The dcerpc session helper also listens on TCP and UDP ports 135.

The session allows FortiOS to handle DCE-RPC dynamic transport address negotiation and to ensure UUID-based security policy enforcement. You can define a security policy to permit all RPC requests or to permit by specific UUID number.

In addition, because a TCP segment in a DCE-RPC stream might be fragmented, it might not include an intact RPC PDU. This fragmentation occurs in the RPC layer; so FortiOS does not support parsing fragmented packets.

The DCE-RPC session helper does not support destination NAT (DNAT) or Firewall VIPs unless you are using the OXID Resolver service (also called IOXIDResolver).

DNS session helpers (dns-tcp and dns-udp)

FortiOS includes two DNS session helpers, dns-tcp, a session helper for DNS over TCP, and dns-udp, a session helper for DNS over UDP.

To accept DNS sessions you must add a security policy with service set to **ALL** or to the DNS pre-defined service (which listens on TCP and UDP ports 53). The dns-udp session helper also listens on UDP port 53. By default the dns-tcp session helper is disabled. If needed you can use the following command to enable the dns-tcp session helper to listen for DNS sessions on TCP port 53:

```
config system session-helper
   edit 0
      set name dns-tcp
      set port 53
      set protocol 6
end
```

File transfer protocol (FTP) session helper (ftp)

The FTP session helper monitors PORT, PASV and 227 commands and NATs the IP addresses and port numbers in the body of the FTP packets and opens ports on the FortiGate unit as required.

To accept FTP sessions you must add a security policy with service set to **ALL** or to the FTP, FTP_Put, and FTP_GET pre-defined services (which all listen on TCP port 21).

H.323 and RAS session helpers (h323 and ras)

The H.323 session helper supports secure H.323 voice over IP (VoIP) sessions between terminal endpoints such as IP phones and multimedia devices. In H.323 VoIP networks, gatekeeper devices manage call registration, admission, and call status for VoIP calls. The FortiOS h323 session helper supports gatekeepers installed on two different networks or on the same network.

To accept H.323 sessions, you must add a security policy with service set to **ALL** or to the H323 pre-defined service (which listens on TCP port numbers 1720 and 1503 and on UDP port number 1719). The h323 session helper listens on TCP port 1720.

The ras session helper is used with the h323 session helper for H.323 Registration, Admission, and Status (RAS) services. The ras session helper listens on UDP port 1719.

Alternate H.323 gatekeepers

The h323 session helper supports using H.323 alternate gatekeepers. All the H.323 endpoints must register with a gatekeeper through the Registration, Admission, and Status (RAS) protocol before they make calls. During the registration process, the primary gatekeeper sends Gatekeeper Confirm (GCF) and Registration Confirm (RCF) messages to the H.323 endpoints that contain the list of available alternate gatekeepers.

The alternate gatekeeper provides redundancy and scalability for the H.323 endpoints. If the primary gatekeeper fails the H.323 endpoints registered with that gatekeeper are automatically registered with the alternate gatekeeper. To use the H.323 alternate gatekeeper, you need to configure security policies that allow H.323 endpoints to reach the alternate gatekeeper.

Media Gateway Controller Protocol (MGCP) session helper (mgcp)

The Media Gateway Control Protocol (MGCP) is a text-based application layer protocol used for VoIP call setup and control. MGCP uses a master-slave call control architecture in which the media gateway controller uses a call agent to maintain call control intelligence, while the media gateways perform the instructions of the call agent.

To accept MGCP sessions you must add a security policy with service set to **ALL** or to the MGCP predefined service (which listens on UDP port numbers 2427 and 2727). The h323 session helper also listens on UDP port numbers 2427 and 2727.

The MGCP session helper does the following:

- VoIP signaling payload inspection. The payload of the incoming VoIP signaling packet is inspected and malformed packets are blocked.

- Signaling packet body inspection. The payload of the incoming MGCP signaling packet is inspected according to RFC 3435. Malformed packets are blocked.
- Stateful processing of MGCP sessions. State machines are invoked to process the parsed information. Any out-of-state or out-of-transaction packet is identified and properly handled.
- MGCP Network Address Translation (NAT). Embedded IP addresses and ports in packet bodies is properly translated based on current routing information and network topology, and is replaced with the translated IP address and port number, if necessary.
- Manages pinholes for VoIP traffic. To keep the VoIP network secure, the IP address and port information used for media or signaling is identified by the session helper, and pinholes are dynamically created and closed during call setup.

ONC-RPC portmapper session helper (pmap)

Open Network Computing Remote Procedure Call (ONC-RPC) is a widely deployed remote procedure call system. Also called Sun RPC, ONC-RPC allows a program running on one host to call a program running on another. The transport address of an ONC-RPC service is dynamically negotiated based on the service's program number and version number. Several binding protocols are defined for mapping the RPC program number and version number to a transport address.

To accept ONC-RPC sessions you must add a security policy with service set to any or to the ONC-RPC pre-defined service (which listens on TCP and UDP port number 111). The RPC portmapper session helper (called pmap) handles the dynamic transport address negotiation mechanisms of ONC-RPC.

PPTP session helper for PPTP traffic (pptp)

The PPTP session help supports port address translation (PAT) for PPTP traffic. PPTP provides IP security at the Network Layer. PPTP consists of a control session and a data tunnel. The control session runs over TCP and helps in establishing and disconnecting the data tunnel. The data tunnel handles encapsulated Point-to-Point Protocol (PPP) packets carried over IP.

To accept PPTP sessions that pass through the FortiGate unit you must add a security policy with service set to all or to the PPTP pre-defined service (which listens on IP port 47 and TCP port 1723). The pptp session helper listens on TCP port 1723.

PPTP uses TCP port 1723 for control sessions and Generic Routing Encapsulation (GRE) (IP protocol 47) for tunneling the encapsulated PPP data. The GRE traffic carries no port number, making it difficult to distinguish between two clients with the same public IP address. PPTP uses the source IP address and the Call ID field in the GRE header to identify a tunnel. When multiple clients sharing the same IP address establish tunnels with the same PPTP server, they may get the same Call ID. The call ID value can be translated in both the control message and the data traffic, but only when the client is in a private network and the server is in a public network.

PPTP clients can either directly connect to the Internet or dial into a network access server to reach the Internet. A FortiGate unit that protects PPTP clients can translate the clients' private IP addresses to a pool of public IP addresses using NAT port translation (NAT-PT). Because the GRE traffic carries no port number for address translation, the pptp session helper treats the Call ID field as a port number as a way of distinguishing multiple clients.

After the PPTP establishing a TCP connection with the PPTP server, the client sends a start control connection request message to establish a control connection. The server replies with a start control connection reply message. The client then sends a request to establish a call and sends an outgoing call request message. FortiOS assigns a Call ID (bytes 12-13 of the control message) that is unique to each PPTP tunnel. The server replies with an outgoing call reply message that carries its own Call ID in bytes 12-13 and the client's call ID in bytes 14-15. The pptp session helper parses the control connection messages for the Call ID to identify the call to which a specific PPP packet belongs. The session helper also identifies an outgoing call request message using the control message type field (bytes 8-9) with the value 7. When the session helper receives this message, it parses the control message for the call ID field (bytes 12-13). FortiOS translates the call ID so that it is unique across multiple calls from the same translated client IP. After receiving outgoing call response message, the session helper holds this message and opens a port that accepts GRE traffic that the PPTP server sends. An outgoing call request message contains the following parts:

- The protocol used for the outgoing call request message (usually GRE)
- Source IP address (PPTP server IP)
- Destination IP address (translated client IP)
- Destination port number (translated client call ID)

The session helper identifies an outgoing call reply message using the control message type field (bytes 8-9) with the value 8. The session helper parses these control messages for the call ID field (bytes 12-13) and the client's call ID (bytes 14-15). The session helper then uses the client's call ID value to find the mapping created for the other direction, and then opens a pinhole to accept the GRE traffic that the client sends.

An outgoing call reply message contains the following parts:

- Protocol used for the outgoing call reply message (usually GRE)
- Source IP address (PPTP client IP)
- Destination IP address (PPTP server IP)
- Destination port number (PPTP server Call ID)

Each port that the session opens creates a session for data traffic arriving in that direction. The session helper opens the following two data sessions for each tunnel:

- Traffic from the PPTP client to the server, using the server's call ID as the destination port
- Traffic from the PPTP server to the client, using the client's translated call ID as the destination port

The default timeout value of the control connection is 30 minutes. The session helper closes the pinhole when the data session exceeds the timeout value or is idle for an extended period.

Remote shell session helper (rsh)

Using the remote shell program (RSH), authenticated users can run shell commands on remote hosts. RSH sessions most often use TCP port 514. To accept RSH sessions you must add a security policy with service set to **ALL** or to the RSH pre-defined service (which listens on TCP port number 514).

FortiOS automatically invokes the rsh session helper to process all RSH sessions on TCP port 514. The rsh session helper opens ports required for the RSH service to operate through a FortiGate unit running NAT or transparent and supports port translation of RSH traffic.

Real-Time Streaming Protocol (RTSP) session helper (rtsp)

The Real-Time Streaming Protocol (RTSP) is an application layer protocol often used by SIP to control the delivery of multiple synchronized multimedia streams, for example, related audio and video streams. Although RTSP is capable of delivering the data streams itself it is usually used like a network remote control for multimedia servers. The protocol is intended for selecting delivery channels (like UDP, multicast UDP, and TCP) and for selecting a delivery mechanism based on the Real-Time Protocol (RTP). RTSP may also use the SIP Session Description Protocol (SDP) as a means of providing information to clients for aggregate control of a presentation consisting of streams from one or more servers, and non-aggregate control of a presentation consisting of multiple streams from a single server.

To accept RTSP sessions you must add a security policy with service set to all or to the RTSP pre-defined service (which listens on TCP ports 554, 770, and 8554 and on UDP port 554). The rtsp session helper listens on TCP ports 554, 770, and 8554.

The rtsp session help is required because RTSP uses dynamically assigned port numbers that are communicated in the packet body when end points establish a control connection. The session helper keeps track of the port numbers and opens pinholes as required. In Network Address Translation (NAT) mode, the session helper translates IP addresses and port numbers as necessary.

In a typical RTSP session the client starts the session (for example, when the user selects the Play button on a media player application) and establishes a TCP connection to the RTSP server on port 554. The client then sends an OPTIONS message to find out what audio and video features the server supports. The server responds to the OPTIONS message by specifying the name and version of the server, and a session identifier, for example, 24256-1.

The client then sends the DESCRIBE message with the URL of the actual media file the client wants to play. The server responds to the DESCRIBE message with a description of the media in the form of SDP code. The client then sends the SETUP message, which specifies the transport mechanisms acceptable to the client for streamed media, for example RTP/RTCP or RDT, and the ports on which it receives the media.

In a NAT configuration the rtsp session helper keeps track of these ports and addresses translates them as necessary. The server responds to the SETUP message and selects one of the transport protocols. When both client and server agree on a mechanism for media transport the client sends the PLAY message, and the server begins streaming the media.

Session Initiation Protocol (SIP) session helper (sip)

The sip session helper is described in the VoIP Solutions: SIP Guide.

Trivial File Transfer Protocol (TFTP) session helper (tftp)

To accept TFTP sessions you must add a security policy with service set to **ALL** or to the TFTP pre-defined service (which listens on UDP port number 69). The TFTP session helper also listens on UTP port number 69.

TFTP initiates transfers on UDP port 69, but the actual data transfer ports are selected by the server and client during initialization of the connection. The tftp session helper reads the transfer ports selected by the TFTP client

and server during negotiation and opens these ports on the firewall so that the TFTP data transfer can be completed. When the transfer is complete the tftp session helper closes the open ports.

Oracle TNS listener session helper (tns)

The Oracle Transparent Network Substrate (TNS) listener listens on port TCP port 1521 for network requests to be passed to a database instance. The Oracle TNS listener session helper (tns) listens for TNS sessions on TCP port 1521. TNS is a foundation technology built into the Oracle Net foundation layer and used by SQLNET.

Advanced concepts

This section provides configuration concepts and techniques to enhance your network security and includes the topics:

- Single firewall vs. multiple virtual domains
- Modem
- FortiExtender
- Assigning IP address by MAC address
- IP addresses for self-originated traffic
- Disk
- CLI scripts
- Rejecting PING requests
- Opening TCP 113
- Obfuscate HTTP responses

To see a collection of practical articles, go to Fortinet's Cookbook site and navigate to **Resources > SysAdmin Notes**.

Single firewall vs. multiple virtual domains

A typical FortiGate setup, with a small to mid-range appliance, enables you to include a number of subnets on your network using the available ports and switch interfaces. This can potentially provide a means of having three or more mini networks for the various groups in a company. Within this infrastructure, multiple network administrators have access to the FortiGate to maintain security policies.

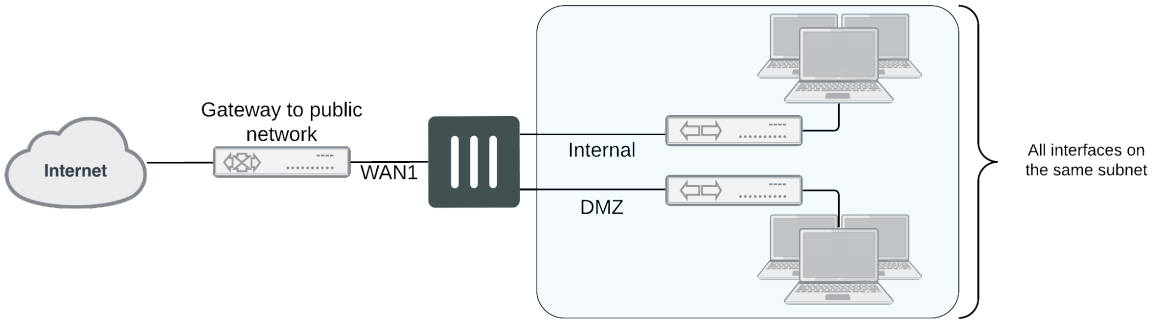
However, the FortiGate unit may not have enough interfaces to match the number of departments in the organization. If the FortiGate unit it running in transparent mode however, there is only one interface, and multiple network branches through the FortiGate are not possible.

A FortiGate unit with Virtual Domains (VDOMs) enabled, provides a means to provide the same functionality in transparent mode as a FortiGate in NAT mode. VDOMs are a method of dividing a FortiGate unit into two or more virtual units that function as multiple independent units. VDOMs can provide separate security policies and, in NAT mode, completely separate configurations for routing and VPN services for each connected network. For administration, an administrator can be assigned to each VDOM, minimizing the possibility of error or fouling network communications.

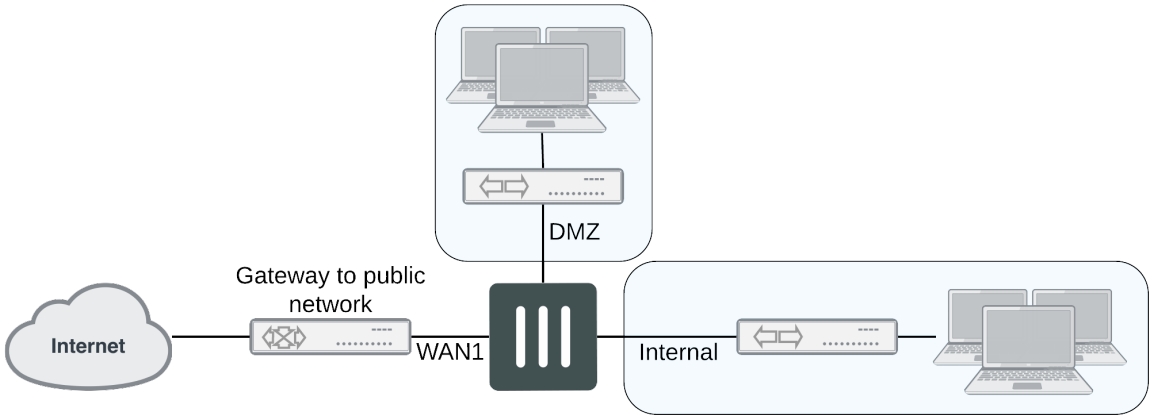
By default, most FortiGate units support 10 VDOMs. Many FortiGate models support purchasing a license key to increase the maximum number.

Single firewall vs. vdoms

When VDOMs are not enabled, and the FortiGate unit is in transparent mode, all the interfaces on your unit become broadcast interfaces. The problem is there are no interfaces free for additional network segments.



A FortiGate with three interfaces means only limited network segments are possible without purchasing more FortiGate devices.



With multiple VDOMs you can have one of them configured in transparent mode, and the rest in NAT mode. In this configuration, you have an available transparent mode FortiGate unit you can drop into your network for troubleshooting, and you also have the standard.

This example shows how to enable VDOMs on the FortiGate unit and the basic and create a VDOM accounting on the DMZ2 port and assign an administrator to maintain the VDOM. First enable Virtual Domains on the FortiGate unit.

To enable VDOMs - web-based manager

1. Go to **System > Dashboard > Status**.
2. In the **System Information** widget, select **Enable** for **Virtual Domain**.

Note that on FortiGate-60 series and lower models, you need to enable VDOMs in the CLI only.

The FortiGate unit logs you out. Once you log back in, you will notice that the menu structure has changed. This reflects the global settings for all Virtual Domains.

To enable VDOMs - CLI

```
config system global
   set vdom-admin enable
end
```

Next, add the VDOM called accounting.

To add a VDOM - web-based manager

1. Go to **Global > VDOM > VDOM**, and select **Create New**.
2. Enter the VDOM name `accounting`.
3. Select **OK**.

To add a VDOM - CLI

```
config vdom
   edit <new_vdom_name>
end
```

With the Virtual Domain created, you can assign a physical interface to it, and assign it an IP address.

To assign physical interface to the accounting Virtual Domain - web-based manager

1. Go to **Global > Network > Interface**.
2. Select the DMZ2 port row and select **Edit**.
3. For the **Virtual Domain** drop-down list, select **accounting**.
4. Select the **Addressing Mode** of **Manual**.
5. Enter the IP address for the port of 10.13.101.100/24.
6. Set the **Administrative Access** to **HTTPS** and **SSH**.
7. Select **OK**.

To assign physical interface to the accounting Virtual Domain - CLI

```
config global
   config system interface
      edit dmz2
      set vdom accounting
      set ip 10.13.101.100/24
      set allowaccess https ssh
   next
end
```

Modem

FortiGate units support the use of wireless, 3G and 4G modems connected using the USB port or, if available, the express card slot. Modem access provides either primary or secondary (redundant) access to the Internet. For FortiGate units that do not include an internal modem (those units with an “M” designation), the modem interface will not appear in the web-based manager until enabled in the CLI. To enable the modem interface enter the CLI commands:

```
config system modem
   set status enable
end
```

You will need to log out of the FortiGate and log back in to see the modem configuration page at **Network > Modem**. Once enabled, modem options become available by going to **Network > Interfaces**.

Note that the modem interface is only available when the FortiGate unit is in NAT mode.

To configure modem settings, go to **> Network > Modem**.

Configuring the modem settings is a matter of entering the ISP phone number, user name and password. Depending on the modem, additional information may need to be supplied such as product identifiers, and initialization strings.

The FortiGate unit includes a number of common modems within its internal database. You can view these by selecting the **Configure Modem** link on the **Modem Settings** page. If your modem is not on the list, select **Create New** to add the information. This information is stored on the device, and will remain after a reboot.

Fortinet has an online database of modem models and configuration settings through FortiGuard. A subscription to the FortiGuard services is not required to access the information. As models are added, you can select the **Configure Modem** link and select **Update Now** to download new configurations.

USB modem port

Each USB modem has a specific dial-out port. This will be indicated with the documentation for your modem. To enable the correct USB port, use the CLI commands:

```
config system modem
   set wireless-port {0 | 1 | 2}
end
```

To test the port, use the diagnose command:

```
diagnose sys modem com /1
```

The 1 will be the value of your USB port selected. The response will be:

```
Serial port: /dev/1
Press Ctrl+W to exit.
```

If the port does not respond the output will be:

```
Can not open modem device '/dev/1' : Broken pipe
```

Modes

The FortiGate unit allows for two modes of operation for the modem; stand alone and redundant. In stand alone mode, the modem connects to a dialup ISP account to provide the connection to the Internet. In redundant mode, the modem acts as a backup method of connecting to the Internet, should the primary port for this function fails.

Configuring either stand alone or redundant modes are very similar. The primary difference is the selection of the interface that the modem will replace in the event of it failing, and the configuration of a PING server to monitor the chosen interface.

Configuring stand alone mode

Configuring stand alone mode is a matter of configuring the modem information and the dialing mode. The dial mode is either **Always Connect** or **Dial on demand**. Selecting **Always Connect** ensures that once the

modem has connected, it remains connected to the ISP. Selecting **Dial on Demand**, the modem only calls the ISP if packets are routed to the modem interface. Once sent, the modem will disconnect after a specified amount of time.

To configure standalone mode as needed - GUI

1. Go to **Network > Modem**.
2. Select the **Mode** of **Standalone**.
3. Select the **Dial Mode** of **Dial on Demand**.
4. Select the number of redials the modem attempts if connection fails to 5.
5. Select **Apply**.

To configure standalone mode as needed- CLI

```
config system modem
   set status enable
   set mode standalone
   set auto-dial enable
   set redial 5
end
```

Configuring redundant mode

Redundant mode provides a backup to an interface, typically to the Internet. If that interface fails or disconnects, the modem automatically dials the configured phone number(s). Once connected, the FortiGate unit routes all traffic to the modem interface until the monitored interface is up again. The FortiGate unit pings the connection to determine when it is back online.

For the FortiGate to verify when the interface is back up, you need to configure a Ping server for that interface. You will also need to configure security policies between the modem interface and the other interfaces of the FortiGate unit to ensure traffic flow.

To configure redundant mode as needed - GUI

1. Go to **Network > Modem**.
2. Select the **Mode** of **Redundant**.
3. Select the interface the modem takes over from if it fails.
4. Select the **Dial Mode** of **Dial on Demand**.
5. Select the number of redials the modem attempts if connection fails to 5.
6. Select **Apply**.

To configure standalone mode as needed- CLI

```
config system modem
   set status enable
   set mode redundant
   set interface wan1
   set auto-dial enable
   set redial 5
end
```

Link Health Monitor

Adding a link health monitor is required for routing fail over traffic. A link health monitor will confirm the connectivity of the device's interface

To add a link health monitor

```
config system link-monitor
   edit "Example1"
      set srcint <Interface_sending_probe>
      set server <ISP_IP_address>
      set protocol <Ping or http>
      set gateway-ip <the_gateway_IP_to_reach_the_server_if_required>
      set failtime <failure_count>
      set interval <seconds>
      set update-cascade-interface enable
      set update-static-route enable
      set status enable
end
```

Additional modem configuration

The CLI provides additional configuration options when setting up the modem options including adding multiple ISP dialing and initialization options and routing. For more information, see the CLI Reference.

Modem interface routing

The modem interface can be used in FortiOS as a dedicated interface. Once enabled and configured, you can use it in security policies and define static and dynamic routing. Within the CLI commands for the modem, you can configure the distance and priority of routes involving the modem interface. The CLI commands are:

```
config system modem
   set distance <route_distance>
   set priority <priority_value>
end
```

For more information on the routing configuration in the CLI, see the CLI Reference. For more information on routing and configuring routing, see the Advanced Routing Guide.

Assigning IP address by MAC address

To prevent users in the from changing their IP addresses and causing IP address conflicts or unauthorized use of IP addresses, you can bind an IP address to a specific MAC address using DHCP.

Use the CLI to reserve an IP address for a particular client identified by its device MAC address and type of connection. The DHCP server then always assigns the reserved IP address to the client. The number of reserved addresses that you can define ranges from 10 to 200 depending on the FortiGate model.

After setting up a DHCP server on an interface by going to **Network > Interfaces**, select the blue arrow next to **Advanced** to expand the options. If you know the MAC address of the system select **Create New** to add it, or if the system has already connected, locate it in the list, select the check box and select **Add from DHCP Client List**.

You can also match an address to a MAC address in the CLI. In the example below, the IP address 10.10.10.55 for User1 is assigned to MAC address 00:09:0F:30:CA:4F.

```
config system dhcp reserved-address
   edit User1
      set ip 10.10.10.55
      set mac 00:09:0F:30:CA:4F
      set type regular
   end
```

IP addresses for self-originated traffic

On the FortiGate unit, there are a number of protocols and traffic that is specific to the internal workings of FortiOS. For many of these traffic sources, you can identify a specific port/IP address for this self-originating traffic. The following traffic can be configured to a specific port/IP address:

- SNMP
- Syslog
- alert email
- FortiManager connection IP
- FortiGuard services
- FortiAnalyzer logging
- NTP
- DNS
- Authorization requests such as RADIUS
- FSSO

Configuration of these services is performed in the CLI. In each instance, there is a command set `source-ip`. For example, to set the source IP of NTP to be on the DMZ1 port with an IP of 192.168.4.5, the commands are:

```
config system ntp
   set ntpsync enable
   set syncinterval 5
   set source-ip 192.168.4.5
end
```

To see which services are configured with source-ip settings, use the get command:

```
get system source-ip status
```

The output will appear similar to the sample below:

```
NTP: x.x.x.x
DNS: x.x.x.x
SNMP: x.x.x.x
Central Management: x.x.x.x
FortiGuard Updates (AV/IPS): x.x.x.x
FortiGuard Queries (WebFilter/SpamFilter): x.x.x.x
```

Disk

To view the status and storage information of the local disk on your FortiGate unit, go to **System > Advanced**. The **DiskSettings** menu appears only on FortiGate units with an internal hard or flash disk.

Formatting the disk

The internal disk of the FortiGate unit (if available) can be formatted by going to **System > Advanced** and selecting **Disk Settings**.

Formatting the disk will erase all data on it, including databases for antivirus and IPS; logs, quarantine files, and WAN optimization caches. The FortiGate unit requires a reboot once the disk has been formatted.

Setting space quotas

If the FortiGate unit has an internal hard or flash disk, you can allocate the space on the disk for specific logging and archiving, and WAN optimization. By default, the space is used on an as required basis. As such, a disk can fill up with basic disk logging, leaving less potential space for quarantine.

By going to **System > Advanced**, you can select the **Edit** icon for **Logging and Archiving** and **WAN Optimization & Web Cache** and define the amount of space each log, archive and WAN optimization has on the disk.

CLI scripts

To upload bulk CLI commands and scripts, go to **System > Advanced**.

Scripts are text files containing CLI command sequences. Scripts can be used to deploy identical configurations to many devices. For example, if all of your devices use identical security policies, you can enter the commands required to create the security policies in a script, and then deploy the script to all the devices which should use those same settings.

Use a text editor such as Notepad or other application that creates simple text files. Enter the commands in sequence, with each line as one command, similar to examples throughout the FortiOS documentation set.

If you are using a FortiGate unit that is not remotely managed by a FortiManager unit or the FortiGuard Analysis and Management Service, the scripts you upload are executed and discarded. If you want to execute a script more than once, you must keep a copy on your management PC.

If your FortiGate unit is configured to use a FortiManager unit, you can upload your scripts to the FortiManager unit, and run them from any FortiGate unit configured to use the FortiManager unit. If you upload a script directly to a FortiGate unit, it is executed and discarded.

If your FortiGate unit is configured to use FortiGuard Analysis and Management Service, scripts you upload are executed and stored. You can run uploaded scripts from any FortiGate unit configured with your FortiGuard Analysis and Management Service account. The uploaded script files appear on the FortiGuard Analysis and Management Service portal web site.

Uploading script files

After you have created a script file, you can then upload it through **System > Advanced**. When a script is uploaded, it is automatically executed.

Commands that require the FortiGate unit to reboot when entered in the command line will also force a reboot if included in a script.

To execute a script

1. Go to **System > Advanced**.
2. Enable **Configuration Scripts**.
3. Select **Upload and Run a New Script** to locate the script file.
4. Select **Apply**.

If the FortiGate unit is not configured for remote management, or if it is configured to use a FortiManager unit, uploaded scripts are discarded after execution. Save script files to your management PC if you want to execute them again later.

If the FortiGate unit is configured to use the FortiGuard Analysis and Management Service, the script file is saved to the remote server for later reuse. You can view the script or run it from the FortiGuard Analysis and Management Service portal web site.

Auto repeat of CLI commands

Occasionally there is a need to repeatedly run a diagnose command over a long period of time (like checking CPU or memory usage, or checking proxy health), Previously, this could only be done with external console connections. With FortiOS 5.4.0, this can be done in a script using the `interval` and `repeat` commands.

Scripts can be uploaded as a file from the CLI or GUI. To upload scripts from the GUI go to **System > Advanced > Configuration Scripts** and upload and run the script.

To configure the schedule and scripts, use the following syntax:

```
config system auto-script
   edit <ScriptName>
      set interval
      set repeat
      set script
   end
end
```

`interval` the interval time in seconds between instances of the script running.

`repeat` the number of times to repeat the running of the script. The value 0 is used to set an infinite number of repetitions.

`start` select `manual` to start the script manually or `auto` to start the script automatically

`script` the contents of the script.

This feature may not be available on all models as a hard drive is necessary to make use of it.

CLI option to limit script output size

The CLI command `set output-size` limits the size of an auto script in megabytes and prevents the memory from being used up by the script's output.

CLI Syntax

```
config system auto-script
   edit <script name>
      set output-size <integer>
   next
end
```

Enter an integer value from 10 to 1024. Default is 10.

Execute restore script command

The `execute restore script` command merges arbitrary configlets into the running configuration from a script. You can carry out the command's authentication with either a username and password or with a certificate.

If the configuration in the script fails for any reason, the system will revert back to running configurations without interrupting the network.

To load script from the FTP, SCP, or TFTP servers, enter the following CLI command:

```
execute restore script {ftp | scp |
    tftp} <dir / filename in server> <server ip> <username> <password>
```

To view the results of the last restored script, enter the following CLI command:

```
execute restore script lastlog <dir / filename in server> <server ip> <username>
    <password>
```

Rejecting PING requests

The factory default configuration of your FortiGate unit allows the default external interface to respond to ping requests. Depending on the model of your FortiGate unit the actual name of this interface will vary. For the most secure operation, you should change the configuration of the external interface so that it does not respond to ping requests. Not responding to ping requests makes it more difficult for a potential attacker to detect your FortiGate unit from the Internet. One such potential threat are Denial of Service (DoS) attacks.

A FortiGate unit responds to ping requests if ping administrative access is enabled for that interface.

To disable ping administrative access - web-based manager

1. Go to **System > Network > Interface**.
2. Choose the external interface and select **Edit**.
3. Clear the **Ping Administrative Access** check box.
4. Select **OK**.

In the CLI, when setting the allowaccess settings, by selecting the access types and not including the PING option, that option is then not selected. In this example, only HTTPS is selected.

To disable ping administrative access - CLI

```
config system interface
   edit external
      set allowaccess https
end
```

Opening TCP 113

Although seemingly contrary to conventional wisdom of closing ports from hackers, this port, which is used for ident requests, should be opened.

Port 113 initially was used as an authentication port, and later defined as an identification port (see RFC 1413). Some servers may still use this port to help in identifying users or other servers and establish a connection. Because port 113 receives a lot of unsolicited traffic, many routers, including on the FortiGate unit, close this port.

The issue arises in that unsolicited requests are stopped by the FortiGate unit, which will send a response saying that the port is closed. In doing so, it also lets the requesting server know there is a device at the given address, and thus announcing its presence. By enabling traffic on port 113, requests will travel to this port, and will most likely, be ignored and never responded to.

By default, the ident port is closed. To open it, use the following CLI commands:

```
config system interface
   edit <port_name>
      set ident_accept enable
end
```

You could also further use port forwarding to send the traffic to a non-existent IP address and thus never have a response packet sent.

Obfuscate HTTP responses from SSL VPN

The FortiGate unit can obfuscate the HTTP responses from SSL VPN servers. By default this option is not enabled. To obfuscate HTTP headers, use the following CLI command:

```
config vpn ssl settings
   set url-obscuration {enable | disable}
end
```

Blocking land attacks in transparent mode

Enabling blocking land attacks allows BFD echo packets to pass through the FortiGate.

Since its a system settings option you can enable or disable blocking land attacks for individual VDOMs if your FortiGate is operating with multiple VDOMs.

Another reason to enable this feature would be if your FortiGate is blocking BFD echo packets that should be allowed to pass through the FortiGate. For example, a FortiGate operating in transparent mode between two routers with a policy that allows all traffic may block BFD echo communication between the routers if blocking land attacks is disabled.

Use the following command to block land attacks and allow BFD echo packets. This option is disabled by default.

Syntax

```
config system settings
   set block-land-attack enable
end
```

Multi-dimension tagging

Multi-dimension tagging is available for address, device, and interface objects.

Tags can be configured in the GUI under **System > Tags**. Once created, these tags can be assigned to network interfaces, addresses, and custom devices and groups. In addition, a **Tags** column has been added for each of these GUI locations, including under **User & Device > Device Inventory**.

Syntax

The `tagging` option is available under `config user device` and `device-group`:

```
config user [device | device-group]
   edit <name>
      config tagging
         edit <name>
            set category <object-tag-name>
            set tags <name>
         next
      end
   next
end
```

The same `tagging` option is also available under `config firewall multicast-address`, `multicast-address6`, `address`, `address6`, `addrgrp`, `addrgrp6`, `proxy-address`, and `config system interface` and `zone` (respectively):

```
config user [multicast-address | multicast-address6 | address | address6 | addrgrp |
    addrgrp6 | proxy-address]
   edit <name>
      config tagging
         edit <name>
            set category <object-tag-name>
            set tags <name>
         next
      end
   next
end
```

```
config system [interface | zone]
   edit <name>
      config tagging
         edit <name>
            set category <object-tag-name>
            set tags <name>
         next
      end
   next
end
```